

Usprawnianie funkcjonowania  
systemu kolejowego  
na rzecz społeczeństwa.

## Przewodnik

### *Wymogi dotyczące systemu zarządzania bezpieczeństwem w zakresie certyfikacji bezpieczeństwa lub autoryzacji bezpieczeństwa*

|                        | <i>Sporządzony przez</i>                                | <i>Zatwierdzony przez</i> | <i>Zaakceptowany przez</i> |
|------------------------|---|---------------------------|----------------------------|
| <i>Imię i nazwisko</i> | S. D'ALBERTANSON<br>C. LAGAIZE DAVOINE<br>A. PATACCHINI | M. SCHITTEKATTE           | B. ACCOU                   |
| <i>Stanowisko</i>      | Specjaliści ds. projektów                               | Kierownik projektu        | Kierownik działu           |
| <i>Data</i>            | 26/04/2021  |                           |                            |
| <i>Podpis</i>          |   |                           |                            |

#### *Historia dokumentu*

| <i>Wersja</i> | <i>Data</i> | <i>Uwagi</i>  |
|---------------|-------------|---|
| 1.0           | 29/6/2018   | Wersja ostateczna do publikacji   |
| 1.1           | 10/7/2018   | Dodana grafika 2, dodany podpis pod grafiką 3.  |
| 1.2           | 04/9/2018   | Zaktualizowano grafikę 2  |
| 1.3           | 26/04/2021  | Zmiany mające na celu odzwierciedlenie zmian w przepisach dotyczących rozporządzenia w sprawie podmiotów odpowiedzialnych za utrzymanie, wprowadzenie odpowiednich odnośników do Europejskiego Kolejowego Modelu Kultury Bezpieczeństwa i z doświadczenia, a także kilka ogólnych poprawek w tekście. |

*Niniejszy dokument stanowi prawnie niewiążące wytyczne Agencji Kolejowej Unii Europejskiej. Pozostaje on bez uszczerbku dla procesów decyzyjnych przewidzianych w obowiązującym ustawodawstwie UE. Ponadto dokonywanie wiążącej wykładni prawa Unii należy do wyłącznych kompetencji Trybunału Sprawiedliwości Unii Europejskiej.*

## 0 Wprowadzenie

Wnioskodawca ubiegający się o jednolity certyfikat bezpieczeństwa lub autoryzację bezpieczeństwa powinien wykazać zgodność z odpowiednimi wymogami dotyczącymi systemu zarządzania bezpieczeństwem określonymi w [rozporządzeniu \(UE\) 2018/762](#). W tym celu powinien przedstawić krajowemu organowi ds. bezpieczeństwa lub, w stosownych przypadkach, Agencji Kolejowej Unii Europejskiej (zwanej dalej „Agencją”) dowód w postaci dokumentu świadczący o ustanowieniu systemu zarządzania bezpieczeństwem, zgodnie z art. 9 [dyrektywy \(UE\) 2016/798](#).

Niniejsze wytyczne stanowią dokument podlegający zmianom opracowany we współpracy z krajowymi organami ds. bezpieczeństwa oraz przedstawicielami sektora, który to dokument ma być ustawicznie udoskonalany w oparciu o informacje zwrotne przekazywane przez użytkowników, biorąc pod uwagę doświadczenia zgromadzone w trakcie wdrażania [dyrektywy \(UE\) 2016/798](#), powiązane wspólne metody oceny bezpieczeństwa (CSM) i wszystkie inne obowiązujące prawa Unii.

### 0.1 Cel przewodnika

Celem niniejszych wytycznych jest:

- *określenie celu każdego z wymogów oceny wskazanych w załączniku I i II wyżej wspomnianych CSM, uzupełnione – jeżeli jest to konieczne – notami wyjaśniającymi, zawierającymi szczegółowe informacje dotyczące poszczególnych terminów lub koncepcji wykorzystanych w wymogach;*
- *wskazanie dowodów, jakie organizacja może przedstawić w celu wykazania zgodności wymaganej w ramach wyżej wspomnianych CSM;*
- *przedstawienie listy przykładów materiałów dowodowych, które można odnotować we wnioskach o jednolity certyfikat bezpieczeństwa lub autoryzacji bezpieczeństwa podczas przeprowadzania oceny, lub które wnioskodawca może wykorzystać jako punkt odniesienia dla swojego wniosku;*
- *przedstawienie przykładowych odniesień i standardów, które mogą pomóc w ocenie, rozwoju, we wdrażaniu lub ciągłym doskonaleniu systemu zarządzania bezpieczeństwem; oraz*
- *zapewnienie wskazówek dotyczących tego, jakie kwestie mogą wymagać rozważenia przez krajowy organ ds. bezpieczeństwa podczas nadzoru nad przedsiębiorstwami kolejowymi lub zarządcami infrastruktury.*

W celu oceny wniosku o jednolity certyfikat bezpieczeństwa obejmujący transport kolejną towarów niebezpiecznych krajowy organ ds. bezpieczeństwa może odgrywać bezpośrednią rolę jako organ właściwy do oceny istotnych części wniosku. Alternatywnie może również pełnić funkcję koordynującą, współdziałając, jeśli będzie to konieczne, z każdym innym organem właściwym w zakresie transportu towarów niebezpiecznych, i występując o opinię tego organu w celu dokonania oceny części wniosku.

### 0.2 Do kogo skierowany jest niniejszy przewodnik?

Niniejszy dokument skierowany jest do:

- *krajowych organów ds. bezpieczeństwa oraz do Agencji Kolejowej Unii Europejskiej, w przypadku gdy oceniają one zgodność systemu zarządzania bezpieczeństwem przedsiębiorstw kolejowych z odpowiednimi wymogami dotyczącymi systemu zarządzania bezpieczeństwem oraz w przypadku, gdy krajowe organy ds. bezpieczeństwa prowadzą nadzór;*
- *krajowych organów ds. bezpieczeństwa w przypadku oceny zgodności systemu zarządzania bezpieczeństwem zarządców infrastruktury z odpowiednimi wymogami dotyczącymi systemu zarządzania bezpieczeństwem oraz w przypadku prowadzenia nadzoru po przyznaniu certyfikatu; oraz*

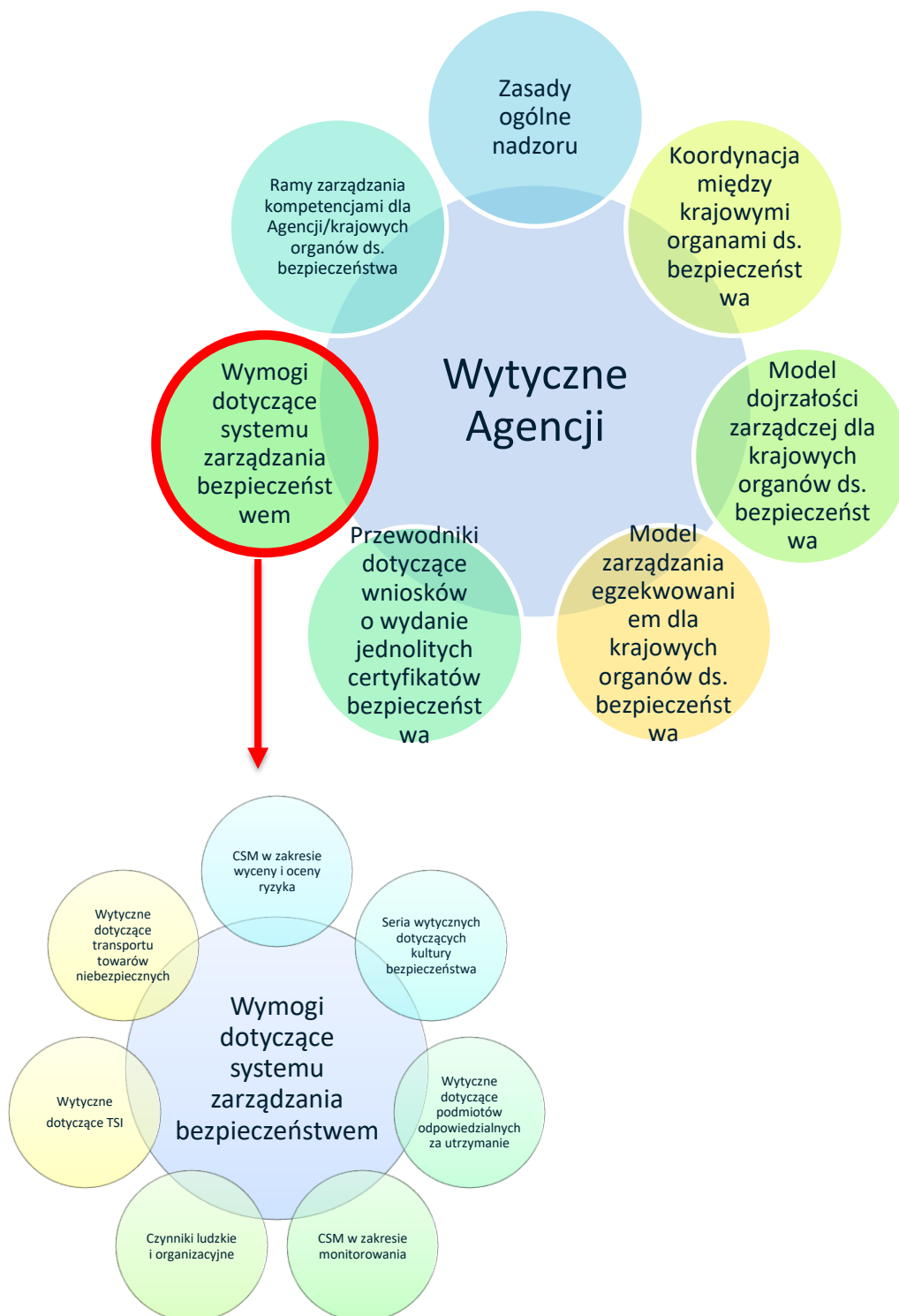
- przedsiębiorstw kolejowych i zarządców infrastruktury (zwanymi dalej również „wnioskodawcami”) w celu udzielenia im wsparcia w opracowywaniu, wdrażaniu, utrzymywaniu i ciągłym doskonaleniu systemu zarządzania bezpieczeństwem, zgodnie z odpowiednimi wymogami dotyczącymi systemu zarządzania bezpieczeństwem (i z innymi obowiązującymi wymogami bezpieczeństwa) oraz aby wiedzieli, czego mogą oczekiwać podczas nadzoru.

### 0.3 Zakres

W niniejszych wytycznych nie określono, jakie dowody powinien przedstawić wnioskodawca. Podstawowym powodem tego jest fakt, że system zarządzania bezpieczeństwem każdej organizacji powinien być dostosowany do określonych czynników ryzyka, które organizacja musi kontrolować. W związku z tym każdy system zarządzania bezpieczeństwem jest niepowtarzalnym systemem udokumentowanych informacji, wskazującym konkretne środki i systemy kontroli ryzyka funkcjonujące w poszczególnych organizacjach, który ewoluuje wraz ze zmianami w danej organizacji. Niewłaściwe byłoby zatem przedstawianie narzuconej listy informacji, które wnioskodawca powinien dostarczyć. Takie postępowanie uczyniłoby proces oceny bezcelowym, ponieważ wszystkie wnioski wyglądałyby tak samo w przeciwieństwie do odpowiednich systemów zarządzania bezpieczeństwem.

### 0.4 Struktura przewodnika

Niniejszy dokument stanowi część kompendium wytycznych Agencji wspierających przedsiębiorstwa kolejowe, zarządców infrastruktury, krajowe organy ds. bezpieczeństwa i Agencję w wypełnianiu funkcji i wykonywaniu zadań zgodnie z [dyrektywą \(UE\) 2016/798](#).



Rys. 1: Kompedium wytycznych Agencji

Informacje przedstawione w niniejszym przewodniku muszą być uzupełnione szczegółowymi wytycznymi krajowych organów ds. bezpieczeństwa, w ramach których określono i wyjaśniono zgłoszone przepisy krajowe obowiązujące w odniesieniu do planowanego obszaru działania oraz dokumenty, które należy zawrzeć we wniosku o jednolity certyfikat bezpieczeństwa w celu zachowania zgodności z przepisami art. 10 ust. 3 lit. b) i art. 10 ust. 8 [dyrektywy \(UE\) 2016/798](#) (zob. również *przewodnik Agencji dotyczący wniosków*

o wydanie jednolitych certyfikatów bezpieczeństwa). Dla zarządców infrastruktury niniejszy przewodnik powinien być uzupełniony o wskazania opracowane przez krajowe organy ds. bezpieczeństwa w zakresie wymagań dot. autoryzacji bezpieczeństwa, jak zostało to przewidziane w art. 12 ust. 1 [dyrektywy \(UE\) 2016/798](#).

Zgłoszone przepisy krajowe oznaczają wyłącznie przepisy zgłoszone Komisji przez państwa członkowskie. Zgodnie z motywem 12 [dyrektywy \(UE\) 2016/798](#) oczekuje się, że z czasem liczba zgłoszonych przepisów krajowych zmniejszy się. Zastąpią je środki określone w technicznych specyfikacjach interoperacyjności (TSI), inne rozporządzenia UE lub zasady firmowe. Firmowe zasady lub normy będą poddawane ocenie, stosownie do potrzeb, pod kątem zgodności z TSI związanymi z podsystemem sieci kolejowej „Ruch kolejowy” w Unii Europejskiej (zwanymi dalej „TSI OPE”), co zostało odzwierciedlone za pośrednictwem wymogów dotyczących systemu zarządzania bezpieczeństwem wyjaśnionych w niniejszym przewodniku.

Struktura niniejszych wytycznych jest zgodna z wymogami określonymi w załączniku I i załączniku II rozporządzenia (UE) 2018/762. W kolejnych sekcjach każdy wymóg umieszczono w żółtej ramce w celu ułatwienia odniesienia. W przypadku różnic między wymogami mającymi zastosowanie do przedsiębiorstw kolejowych a wymogami mającymi zastosowanie do zarządców infrastruktury odpowiedni tekst dotyczący drugiego przypadku pojawi się w żółtych ramkach zawierających wymogi w kolorze [niebieskim](#).

Szczegółowe porównanie lub tabele korelacji między kryteriami oceny poprzednich rozporządzeń (UE) nr 1158/2010 i (UE) nr 1169/2010 a wymogami [rozporządzenia \(UE\) 2018/762](#) zawiera Załącznik 1 do niniejszego przewodnika. W stosownych przypadkach tabele zawierają również odniesienia do punktów ISO High Level Structure. Uwzględnia się je, aby pomóc wnioskodawcom wykazać zgodność ich systemów zarządzania bezpieczeństwem z nowymi wymogami, w szczególności w przypadkach, gdy wnioskodawcy wydano już certyfikat bezpieczeństwa lub autoryzację bezpieczeństwa lub gdy wnioskodawca dysponuje kolejnym systemem zarządzania ISO (np. ISO 9001, 14001 lub 45001) – aby możliwe było zintegrowanie tych systemów – lub planuje opracować system, wykorzystując ten model. Stosowanie tej tabeli nie stanowi regularnego domniemania zgodności z wymogami określonymi w [rozporządzeniu \(UE\) 2018/762](#) w odniesieniu do organizacji posiadających certyfikat ISO.

## 0.5 Dyrektywy ISO/IEC, część 1, Skonsolidowany Supplement ISO

ISO opracowała oficjalne procedury, które należy stosować w przypadku opracowywania i utrzymywania międzynarodowej normy. W dodatku 2 załącznika SL do [dyrektyw ISO/IEC, części 1, Skonsolidowanego suplementu ISO](#) przyjęto High Level Structure (HLS) w celu stosowania tekstu głównego w każdej normie dotyczącej systemu zarządzania.

W załączniku I i załączniku II do rozporządzenia (UE) 2018/762 zapewnia się strukturę zgodną z ISO HLS, ułatwiając – w stosownych przypadkach – integrację różnych systemów zarządzania bezpieczeństwem, w ramach których obowiązują te same główne zasady i wymogi organizacyjne, lecz obszar zgodności z prawem i obszar ryzyka różnią się w zależności od dziedziny (np. bezpieczeństwa, środowiska, jakości pracy).

Normy ISO i odpowiednie wytyczne mogą pomóc przedsiębiorstwom kolejowym i zarządcom infrastruktury w opracowywaniu systemu zarządzania bezpieczeństwem (np. ISO 31000 jest powszechnym dokumentem służącym lepszemu zrozumieniu zarządzania ryzykiem, ISO 31010 dostarcza informacje dotyczące wyboru i stosowania technik oceny ryzyka, takich jak FMECA, FTA, ETA, HAZOP, norma ISO 55000 zawiera wymogi dotyczące zarządzania aktywami). Mogą one jednak być przydatne jedynie w przypadku dysponowania gruntowną wiedzą na temat kontekstu czynników ryzyka związanych z koleją.

Jeżeli wykorzystanie struktury HLS zapewnia postawę zgodną z normami ISO dotyczącymi systemu zarządzania, należy podkreślić, że wyżej wspomniane CSM są regulacjami, które w pierwszej kolejności służą do celów krajowych organów ds. bezpieczeństwa lub Agencji w zakresie oceny wniosków o wydanie

certyfikatów bezpieczeństwa lub autoryzacji bezpieczeństwa. Oceny dotyczące jednolitych certyfikatów bezpieczeństwa lub autoryzacji bezpieczeństwa będą przeprowadzane pod kątem wymogów dotyczących systemu zarządzania bezpieczeństwem, a nie pod kątem struktury ISO HLS jako takiej. Innymi słowy, normy ISO opierają się na dobrowolnej certyfikacji, ale niektóre ramy prawne uwzględniają je w celu zapewnienia domniemania zgodności z obowiązującymi przepisami regulującymi daną dziedzinę. Nie istnieje przepis przyznający normom ISO domniemanie zgodności z wymogami określonymi w [dyrektywie \(UE\) 2016/798](#) lub [rozporządzeniu \(UE\) 2018/762](#).

Punkty 4–10.2 zaczerpnięte z dyrektyw ISO/IEC, część 1 oraz ze skonsolidowanego suplementu z 2016 r., załącznika SL, dodatku 2 są odtworzone lub przystosowane za zgodą Międzynarodowej Organizacji Normalizacyjnej, ISO. Aby zapoznać się z oryginalnym tekstem, należy odnieść się do dokumentu źródłowego. Dokument ten można uzyskać na [stronie internetowej Centralnego Sekretariatu ISO](#). Prawa autorskie zachowuje ISO.

## 0.6 Cel systemu zarządzania bezpieczeństwem

Celem systemu zarządzania bezpieczeństwem jest zapewnienie, aby dana organizacja kontrolowała ryzyko, które powstaje w konsekwencji działalności przedsiębiorstwa, w bezpieczny sposób oraz aby spełniała wszystkie obowiązki w zakresie bezpieczeństwa odnoszące się do niej.

Stosowanie uporządkowanego podejścia umożliwia identyfikację zagrożeń oraz stałą kontrolę ryzyka związanego z działalnością danej organizacji, co ma na celu zapobieganie wypadkom. W ramach tego podejścia uwzględniono ryzyko wspólne na płaszczyźnie oddziaływań pomiędzy podmiotami w systemie kolejowym (głównie między przedsiębiorstwami kolejowymi, zarządcami infrastruktury i podmiotami odpowiedzialnymi za utrzymanie, lecz również wszystkimi innymi podmiotami mającymi potencjalny wpływ na bezpieczne działanie systemu kolej, takimi jak producenci, dostawcy usług utrzymania, dysponenci, usługodawcy, podmioty zamawiające, przedsiębiorstwa kolejowe, nadawcy, odbiorcy, załadowcy, rozładowcy, ośrodki szkoleniowe, pasażerowie i inne osoby mające styczność z systemem kolejowym itd.). Odpowiednie wdrożenie wszystkich właściwych elementów systemu zarządzania bezpieczeństwem daje organizacji niezbędną pewność, że w każdych warunkach kontroluje ona i będzie stale kontrolować wszystkie zidentyfikowane rodzaje ryzyka związane z jej działalnością.

Dojrzałe organizacje są świadome tego, że proces skutecznej kontroli ryzyka jest możliwy tylko przy zintegrowaniu trzech kluczowych parametrów: czynnika technicznego obejmującego stosowane narzędzia i wyposażenie, czynnika ludzkiego obejmującego bezpośrednio zaangażowanych pracowników oraz ich umiejętności, wyszkolenie i motywację, a także czynnika organizacyjnego, obejmującego procedury i metody określające zależności pomiędzy zadaniami.

W rezultacie odpowiedni system zarządzania bezpieczeństwem skutecznie monitoruje i przyczynia się do ulepszenia wszystkich trzech parametrów jego środków kontroli ryzyka. Wiele cech kolejowego systemu zarządzania bezpieczeństwem jest bardzo podobnych do praktyk zarządzania zalecanych przez zwolenników jakości, zdrowia i bezpieczeństwa w pracy, ochrony środowiska i doskonałości biznesowej. W związku z tym, jak wskazano powyżej, zasady dobrego zarządzania można łatwiej zintegrować, stosując CSM oparte na strukturze ISO HLS, przez co całkowita reorganizacja organizacji, które posiadają już takie systemy, może nie być potrzebna.

Uznano, że uporządkowane systemy zarządzania stanowią wartość dodaną przedsiębiorstwa dzięki skutecznemu zarządzaniu powiązaniem. Pomoże to poprawić ogólną wydajność, wprowadzić udoskonalenia operacyjne, poprawić stosunki z wykonawcami i podwykonawcami, klientami i organami regulacyjnymi, a także pomoże w budowaniu pozytywnej kultury bezpieczeństwa.

Wnioskodawca musi opracować swój system zarządzania bezpieczeństwem w taki sposób, aby zachować zgodność z wymogami określonymi w art. 9 [dyrektywy \(UE\) 2016/798](#) w celu zapewnienia bezpiecznego

zarządzania działaniami. W tym celu wnioskodawca musi wykazać zgodność z wymogami określonymi w załącznikach I i II [rozporządzenia \(UE\) 2018/762](#). Wymogi te opracowano w taki sposób, aby przedstawiały pełny obraz systemu zarządzania bezpieczeństwem organizacji zgodnego z cyklem planuj-wykonaj-sprawdź-działaj (PDCA). Wnioskodawca będzie musiał uwzględnić każdy indywidualny wymóg, a także sposób, w jaki pasują one do siebie, tworząc spójny system zarządzania bezpieczeństwem, kontrolujący istotne rodzaje ryzyka.

## 0.7 System zarządzania bezpieczeństwem i podejście procesowe

System zarządzania bezpieczeństwem jest środkiem pozwalającym na połączenie wielu aspektów działalności w celu zapewnienia organizacji zdolności do jej prowadzenia w sposób bezpieczny i skuteczny. Te połączone odpowiednio elementy pozwolą na zagwarantowanie zgodności z międzynarodowymi i krajowymi regulacjami i normami, wymaganiami sektorowymi i biznesowymi, jak również wynikami oceny ryzyka oraz na zastosowanie dobrych praktyk we wszystkich aspektach działalności przedsiębiorstwa. Dla tych celów system zarządzania bezpieczeństwem powinien zostać włączony w procesy biznesowe organizacji, a nie stać się tylko systemem „papierowym”, opracowanym wyłącznie dla wykazania zgodności z wymaganiami regulacyjnymi. System zarządzania bezpieczeństwem powinien być „żywym” zestawem ustaleń, który dojrzewa i rozwija się jak organizacja, której służy. Stworzenie systemu zarządzania bezpieczeństwem wymaga od organizacji zrozumienia zagrożeń, które musi kontrolować, ram prawnych, w których działa, oraz posiadania jasnej wizji oczekiwanych wyników. Niniejszy przewodnik wskazuje elementy systemu zarządzania bezpieczeństwem, które koniecznie będą musiały zostać spełnione, aby organ oceniający mógł wydać jednolity certyfikat bezpieczeństwa. Podkreślić jednocześnie należy, że jakość systemu zarządzania bezpieczeństwem wykracza poza sumę jego części. System zarządzania bezpieczeństwem musi funkcjonować jako spójna całość, w której zgodność elementów zapewnia jej prawidłowe działanie.

Wymogi, pod kątem których dokonywana będzie ocena systemu zarządzania bezpieczeństwem, mogą zostać spełnione w drodze udokumentowanego procesu (lub procedury itp.), należy je jednak również zintegrować w ramach różnych obszarów biznesowych organizacji. Na przykład krajowy organ ds. bezpieczeństwa może sprawdzić, czy istnieje deklaracja w zakresie stosowanej polityki, ale musi również zweryfikować zobowiązanie organizacji do jej stosowania. Z praktycznego punktu widzenia krajowy organ ds. bezpieczeństwa może dokonać tego, sprawdzając sposób monitorowania i przeprowadzania przeglądów systemu zarządzania bezpieczeństwem na poziomie kadry kierowniczej wyższego szczebla, weryfikując sposób, w jaki pracownicy są zaangażowani w ten proces oraz sposób przekazywania im rezultatów. Podobnie organizacja może nie dysponować określoną procedurą lub procedurami w zakresie zarządzania informacjami związanymi z bezpieczeństwem, ale musi określić sposób, w jaki właściwe części przedsiębiorstwa zarządzają nimi w odpowiedni sposób (np. przekazywanie informacji związanych z bezpieczeństwem maszyniście).

Ważna zmiana uwzględniona w załączniku I i załączniku II do [rozporządzenia \(UE\) 2018/762](#) jest wstępem do podejścia procesowego. Podejście to jest również promowane w normach ISO dotyczących systemu zarządzania, w ramach których różne procesy systemu zarządzania są ściśle powiązane, a ich spójne działanie przyczynia się do osiągnięcia celów organizacji. W załączniku I i załączniku II do [rozporządzenia \(UE\) 2018/762](#) określono pewne istotne powiązania między procesami w celu ułatwienia zrozumienia podejścia procesowego; nie oznacza to jednak, że są to jedyne powiązania ani że powinny być wykazywane do celów zapewnienia zgodności. Zdolność organizacji do przedstawienia sposobu, w jaki procesy systemu zarządzania łączą się ze sobą, jest dobrym wskaźnikiem zrozumienia przez organizację sposobu skutecznego działania jej systemu zarządzania.

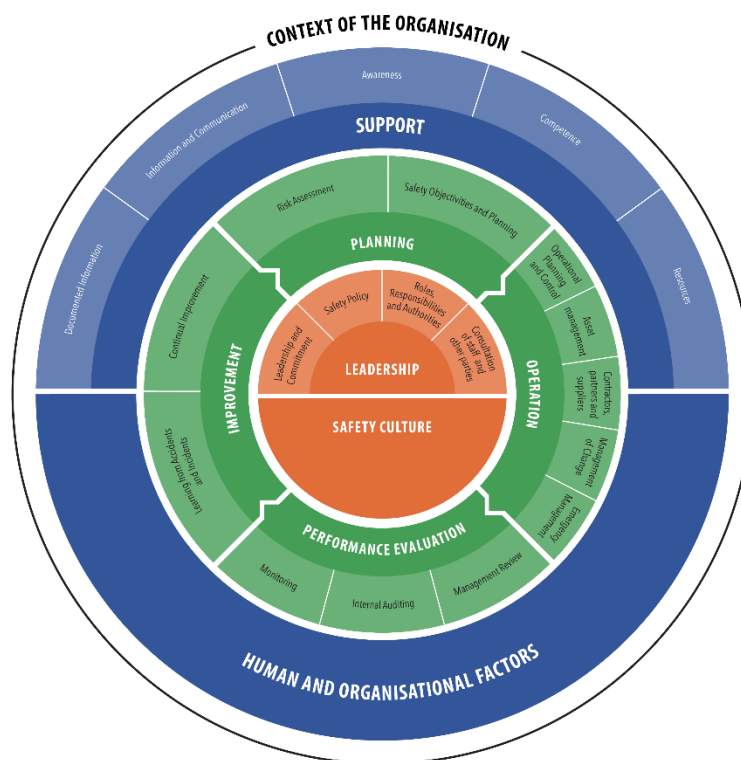
Można zaobserwować, że elementy systemu zarządzania bezpieczeństwem działają zgodnie z cyklem planuj-wykonaj-sprawdź-działaj (PDCA) (zob. Rys. 2). Koncepcja PDCA odzwierciedla powiązania funkcjonalne między głównymi elementami systemu zarządzania bezpieczeństwem:



- **planowanie:** identyfikowanie ryzyka i możliwości, ustalenie celów w zakresie bezpieczeństwa oraz określenie procesów i środków niezbędnych do osiągnięcia wyników zgodnie ze strategią organizacji w zakresie bezpieczeństwa;
- **funkcjonowanie:** opracowanie, wdrażanie i stosowanie procesów i środków zgodnie z planem;
- **ocena wyników:** monitorowanie i ocena wydajności wdrożonych procesów i środków w odniesieniu do celów i planowania oraz zgłaszanie wyników;
- **doskonalenie:** podejmowanie działań służących ciągłemu doskonaleniu systemu zarządzania bezpieczeństwem i poprawie skuteczności działania w zakresie bezpieczeństwa w celu osiągnięcia zamierzonych wyników.

Ten podstawowy proces PDCA jest uzupełniony innymi elementami systemu zarządzania bezpieczeństwem:

- „kontekst organizacji” dostarcza informacje niezbędne dla fazy planowania;
- „przywództwo” jako siła napędowa cyklu PDCA;
- różne funkcje „wsparcia” stanowiące pomoc dla wszystkich elementów systemu zarządzania bezpieczeństwem.



Rys. 2: System zarządzania bezpieczeństwem na kolei

## 0.8 System zarządzania bezpieczeństwem, czynniki ludzkie i organizacyjne oraz kultura bezpieczeństwa

Czynniki ludzkie i organizacyjne łączą wiedzę z zakresu nauk społecznych, takich jak: nauki o zarządzaniu, psychologia, socjologia, nauki o projektowaniu, nauki polityczne, w celu poszerzenia zakresu badań przy uwzględnieniu organizacyjnych, instytucjonalnych, kulturowych i politycznych czynników wpływających na

bezpieczeństwo. Według Międzynarodowego Stowarzyszenia Ergonomicznego ergonomia (lub czynniki ludzkie) to dyscyplina naukowa zajmująca się zrozumieniem interakcji między ludźmi a innymi elementami systemu oraz zawód polegający na stosowaniu teorii, zasad, danych i innych metod w projektowaniu w celu optymalizacji dobrostanu ludzi i ogólnej wydajności systemu (zob. również definicja – Załącznik 6).

Termin „organizacyjne” został wprowadzony w celu podkreślenia nadrzędnego, organizacyjnego poziomu analizy, a nie tylko poziomu indywidualnego, choć oczywiście organizacje składają się z jednostek.

Badanie czynników ludzkich i organizacyjnych jest częścią procesu zarządzania bezpieczeństwem, przy czym (pozytywna) kultura bezpieczeństwa jest częścią wyniku (lub rezultatu) tego procesu.

Kultura bezpieczeństwa jest zestawem wzorców zachowań i myślenia, które w dużej mierze dzielone są w ramach organizacji, w odniesieniu do zarządzania istotnym ryzykiem związanym z ich działalnością. Zakłada się oczywiście, że w ramach organizacji mogą występować różne kultury bezpieczeństwa, zależnie od pełnionej funkcji, geografii lub innych dzielonych wartości. W związku z tym kultura bezpieczeństwa rozwija się na bieżąco przez interakcje między podmiotami w kontekście organizacji, która musi dostosować się do jej otoczenia (zob. również definicja – Załącznik 6).

Podsumowując, aby w bezpośredni sposób opisać kulturę bezpieczeństwa, należy przyjrzeć się czynnikom kształtującym zachowanie. System zarządzania bezpieczeństwem stanowi podstawę: w ramach określania przypuszczalnych warunków pracy i oczekiwanych wyników organizacja określi preferowany sposób pracy oraz środki techniczne służące wsparciu działania. Aby bezpiecznie funkcjonować, organizacja przewidzi niekorzystne sytuacje i zastosuje zasady i środki, aby im zaradzić. Ponadto istnieje „świat ludzki” organizacji: cechy, uczucia, znaczenia i powiązania warunkujące wzorce interakcji między jednostkami w ramach organizacji w taki sposób, aby wpływały na sposób myślenia i zachowania. Ta kulturowa strona odnosi się głównie do „niepisanych zasad regulujących zachowanie i decyzje grupy ludzi”. Łącznie aspekt strukturalny i kulturowy organizacji ułatwia (lub utrudnia) funkcjonowanie organizacji.

Istnieje jednak duże ryzyko, że zbyt biurokratyczne podejście do zarządzania bezpieczeństwem będzie sprzeczne z faktycznymi warunkami operacyjnymi i w rezultacie system zarządzania bezpieczeństwem zacznie żyć własnym życiem, tj. wszystkie wysiłki zostaną włożone w opracowywanie, utrzymywanie, a nawet dowodzenie istnienia udokumentowanego systemu, przy jednoczesnym ignorowaniu informacji operacyjnych niezbędnych do zapewnienia jego działania zgodnego z przeznaczeniem oraz tworzeniu znacznych niezgodności między „funkcjonowaniem zgodnym z wyobrażeniem” a „faktycznym funkcjonowaniem”.

Z drugiej strony istnieje możliwość wdrożenia systemu zarządzania bezpieczeństwem jako instrumentu w celu wywarcia pozytywnego wpływu na kulturę bezpieczeństwa organizacji oraz na środowisko fizyczne i zachowanie pracowników w sposób promujący i ułatwiający bezpieczeństwo. Jest to połączenie aspektu strukturalnego i kulturowego organizacji, które w rezultacie przyczynia się do zapewnienia bezpieczeństwa. Tu istotną rolę powinny odgrywać czynniki ludzkie i organizacyjne. Aby pomóc ludziom w wypełnianiu ich zadania, organizacja musi zrozumieć sposób, w jaki ludzie (z ich zdolnościami i ograniczeniami) wykorzystują zasoby (np. wyposażenie kabiny maszynisty lub dowolny interfejs człowiek-maszyna) i specyfikacje do rozwiązywania problemów, oraz musi uwzględnić tę wiedzę przy kształtowaniu ich środowiska pracy. Dotyczy to również zasad i przepisów: tak długo, jak pracownicy realizujący swoje zadania nie będą uwzględniani w opracowywaniu procedur dotyczących pracy, będą zmuszeni łamać zasady, aby wykonać pracę, niezależnie od pojawiających się sprzeczności lub konfliktów.

Agencja, wraz z przedstawicielami sektora, opracowała [Europejski Kolejowy Model Kultury Bezpieczeństwa \(ERSCM\)](#), który przedstawiono w części Załącznik 4 (tłumaczenia wytycznych dotyczących ERSCM można znaleźć we wszystkich językach UE na stronie internetowej Agencji Kolejowej Unii Europejskiej, do której to strony link znajduje się w załączniku 4). W niniejszym dokumencie w odpowiedni sposób wyjaśniono czynniki ludzkie i organizacyjne oraz podstawowe cechy, o których wiadomo, że przyczyniają się do zapewnienia pozytywnej kultury bezpieczeństwa. Ponadto w częściach Załącznik 4 i Załącznik 5 przedstawiono inne

informacje przydatne dla organizacji przy opracowywaniu własnych strategii. Czytelnikom przypomina się, że mogą swobodnie stosować własne modele kultury bezpieczeństwa w celu wypełnienia swoich zobowiązań prawnych.

## 0.9 Dowody potwierdzające i dokumentacja

W niniejszym dokumencie przedstawiono wskazówki dotyczące dowodów, które wnioskodawca (tj. przedsiębiorstwo kolejowe lub zarządca infrastruktury) musi dostarczyć, ubiegając się o certyfikat bezpieczeństwa lub autoryzację bezpieczeństwa, z powodów wymienionych powyżej nie wskazano jednak dokładnie, jakie dowody należy dostarczyć. W odniesieniu do każdego wymogu wskazano dowody, jakie wnioskodawca powinien dostarczyć wraz z odpowiednim odniesieniem do tego wymogu. Ponadto przedstawiono przykłady takich dowodów w praktyce. Należy uwzględnić fakt, że przykłady podano jako pomoc w zrozumieniu określonych kwestii i nie są one jedynym sposobem wykazania zgodności ani nie stanowią pełnej listy możliwych alternatyw. Ponadto należy zrozumieć, że w przypadku gdy wnioskodawca składa wniosek, opisuje on, w jaki sposób spełnia każdy wymóg. Podmiot oceniający lub wnioskodawca może zwrócić się o dostarczenie dowodów lub może dostarczyć dowody w postaci sugerowanych informacji w celu wyjaśnienia lub poparcia sposobu spełnienia wymogów. W przypadku wnioskodawcy i podmiotu oceniającego najważniejszym punktem dotyczącym każdego wymogu jest dopilnowanie, aby oświadczenia dotyczące zgodności były powiązane z odniesieniami, w ramach których wyjaśniono, gdzie można znaleźć dalsze dowody potwierdzające złożone oświadczenie. W sekcji przykładów dotyczących każdego wymogu podjęto próbę określenia, jak mógłby wyglądać taki przywołany materiał.

Odniesienia, które powinny być pomocne dla wnioskodawców podczas opracowywania wniosku, wymieniono na końcu niniejszej sekcji. Ponadto w ramach ostatniej sekcji, pod każdym jej elementem podjęto próbę stworzenia niezbędnego łączy odsyłającego do Nadzoru. W sekcji tej wskazano kwestie, jakie podmiot oceniający mógłby zechcieć przedstawić zespołom krajowych organów ds. bezpieczeństwa odpowiedzialnym za nadzór jako obszary zainteresowania, które mogłyby zostać wykorzystane do zbadania kompleksowości systemu zarządzania bezpieczeństwem.

Podobnie jak podejście wprowadzone w ramach norm ISO dotyczących systemu zarządzania, załącznik I i załącznik II do rozporządzenia (UE) 2018/762 nie mają charakteru nakazowego – z wyjątkiem szczególnych przypadków – w odniesieniu do charakteru dowodów (np. procedury) oczekiwanych od wnioskodawcy. Elastyczność pozostawiona wnioskodawcy pozwala organizacjom przedstawić swoje ustalenia związane z systemem zarządzania bezpieczeństwem w sposób odzwierciedlający charakter działalności i proporcjonalny do jej skali. Ponadto pomoże w odchodzeniu od testu zgodności w formie papierowej w kierunku oceny żywego, rozwijającego się systemu, która we właściwy sposób odzwierciedli faktyczne ustalenia przedsiębiorstwa w zakresie zarządzania bezpieczeństwem.

Termin „dokumentacja” został wprowadzony w ramach struktury ISO HLS oraz jako wspólny termin dla norm dotyczących systemu zarządzania. Definicja „dokumentacji” znajduje się w *punkcie 3.8 normy ISO 9000*. Dokumentację można wykorzystać do przekazywania wiadomości, dostarczania dowodów dotyczących planowanych i faktycznie wykonanych działań lub do dzielenia się wiedzą. Dokumentacja obejmuje między innymi dokumenty i rejestry, takie jak procedury, protokoły z posiedzeń, sprawozdania, oficjalne komunikaty dotyczące celów, wyniki, porozumienia, umowy itp. Dalsze wyjaśnienia znajdują się w *Wytycznych w sprawie wymogów dotyczących udokumentowanych informacji ISO 9001:2015* dostępnych na [stronie internetowej ISO](#).

Termin „procedura” nie powinien sugerować istnienia samodzielnego dokumentu, obejmując wyłącznie i w wyczerpujący sposób zarządzanie każdym pojedynczym elementem systemu zarządzania bezpieczeństwem, ani wymagać opracowania szczególnego zestawu nowych dokumentów. Odniesienie w niniejszym dokumencie do procedury oznacza dokumentację (np. dokumenty w formie papierowej)

określającą etapy, które należy stosować. Odniesienie do procesu oznacza odniesienie do środków służących wykonaniu zadania lub osiągnięciu celu, które mogą, ale nie muszą być określone w procedurze.

## 0.10 Odniesienia do innych rozporządzeń UE i obowiązujących wymogów prawnych

Odniesienia do innych rozporządzeń UE przyczyniają się do zwiększenia spójności między różnymi tekstami prawnymi, potwierdzając powiązania między nimi. Ustalenia dotyczące systemu zarządzania bezpieczeństwem powinny być zawsze zgodne z obowiązującym tekstem prawnym, o ile nie określono inaczej (np. szczególne przepisy przejściowe, spóźniony wniosek). W przypadku uchylecia rozporządzenia UE, wszystkich odniesień zazwyczaj dokonuje się w stosunku do nowego rozporządzenia (o ile w rozporządzeniu nie określono inaczej).

Wszystkie przedsiębiorstwa kolejowe i wszyscy zarządcy infrastruktury muszą przestrzegać szeregu zobowiązań prawnych, których zakres wykracza poza zobowiązania związane wyłącznie z kwestiami bezpieczeństwa. Niektóre inne zobowiązania będą miały bezpośredni lub pośredni wpływ na sposób, w jaki organizacje wypełniają swoje obowiązki w zakresie bezpieczeństwa w ramach swojego systemu zarządzania bezpieczeństwem, np. zachowanie zgodności z przepisami [dyrektywy \(UE\) 2016/797](#) (dyrektywy w sprawie interoperacyjności) lub znaczenie bezpieczeństwa usług świadczonych przez zarządców infrastruktury na rzecz przedsiębiorstw kolejowych w ramach [dyrektywy \(UE\) 2012/34](#). W związku z tym system zarządzania bezpieczeństwem stosowany przez przedsiębiorstwa kolejowe i zarządców infrastruktury w celu przeciwdziałania zagrożeniom dla bezpieczeństwa musi być uporządkowany, aby w stosownych przypadkach zapewnić zgodność z innymi zobowiązaniami prawnymi.

Usprawnianie funkcjonowania  
systemu kolejowego  
na rzecz społeczeństwa.

## Spis treści

|       |   |    |
|-------|---|----|
| 0     | Wprowadzenie .....  | 3  |
| 0.1   | Cel przewodnika .....   | 3  |
| 0.2   | Do kogo skierowany jest niniejszy przewodnik? .....   | 3  |
| 0.3   | Zakres .....  | 4  |
| 0.4   | Struktura przewodnika .....   | 4  |
| 0.5   | Dyrektywy ISO/IEC, część 1, Skonsolidowany Suplement ISO .....  | 6  |
| 0.6   | Cel systemu zarządzania bezpieczeństwem .....   | 7  |
| 0.7   | System zarządzania bezpieczeństwem i podejście procesowe .....  | 8  |
| 0.8   | System zarządzania bezpieczeństwem, czynniki ludzkie i organizacyjne oraz kultura<br>bezpieczeństwa ..... | 9  |
| 0.9   | Dowody potwierdzające i dokumentacja .....  | 11 |
| 0.10  | Odniesienia do innych rozporządzeń UE i obowiązujących wymogów prawnych .....                             | 12 |
| 1     | Kontekst organizacji .....  | 18 |
| 1.1   | Wymóg regulacyjny .....   | 18 |
| 1.2   | Cel .....   | 18 |
| 1.3   | Noty wyjaśniające .....   | 19 |
| 1.4   | Dowody .....  | 20 |
| 1.5   | Przykłady dowodów .....   | 21 |
| 1.6   | Odniesienia i normy .....   | 23 |
| 1.7   | Kwestie związane z nadzorem .....   | 23 |
| 2     | Przywództwo .....   | 24 |
| 2.1   | Przywództwo i zaangażowanie .....   | 24 |
| 2.1.1 | Wymóg regulacyjny .....   | 24 |
| 2.1.2 | Cel .....   | 24 |
| 2.1.3 | Noty wyjaśniające .....   | 25 |
| 2.1.4 | Dowody .....  | 25 |
| 2.1.5 | Przykłady dowodów .....   | 26 |
| 2.1.6 | Odniesienia i normy .....   | 27 |
| 2.1.7 | Kwestie związane z nadzorem .....   | 27 |
| 2.2   | Strategia w zakresie bezpieczeństwa .....   | 28 |
| 2.2.1 | Wymóg regulacyjny .....   | 28 |
| 2.2.2 | Cel .....   | 28 |
| 2.2.3 | Noty wyjaśniające .....   | 28 |
| 2.2.4 | Dowody .....  | 29 |
| 2.2.5 | Przykłady dowodów .....   | 29 |

|       |  |    |
|-------|--|----|
| 2.2.6 | Kwestie związane z nadzorem .....  | 30 |
| 2.3   | Funkcje, odpowiedzialność, rozliczalność i uprawnienia w ramach organizacji..... | 31 |
| 2.3.1 | Wymóg regulacyjny.....   | 31 |
| 2.3.2 | Cel.....   | 31 |
| 2.3.3 | Noty wyjaśniające .....  | 31 |
| 2.3.4 | Dowody .....   | 32 |
| 2.3.5 | Przykłady dowodów .....  | 33 |
| 2.3.6 | Odniesienia i normy .....  | 34 |
| 2.3.7 | Kwestie związane z nadzorem .....  | 34 |
| 2.4   | Konsultacje z pracownikami i innymi stronami.....                                | 35 |
| 2.4.1 | Wymóg regulacyjny.....   | 35 |
| 2.4.2 | Cel.....   | 35 |
| 2.4.3 | Noty wyjaśniające .....  | 35 |
| 2.4.4 | Dowody .....   | 36 |
| 2.4.5 | Przykłady dowodów .....  | 36 |
| 2.4.6 | Kwestie związane z nadzorem .....  | 36 |
| 3     | Planowanie.....  | 38 |
| 3.1   | Działania mające na celu ograniczenie ryzyka .....                               | 38 |
| 3.1.1 | Wymóg regulacyjny.....   | 38 |
| 3.1.2 | Cel.....   | 39 |
| 3.1.3 | Noty wyjaśniające .....  | 39 |
| 3.1.4 | Dowody .....   | 41 |
| 3.1.5 | Przykłady dowodów .....  | 42 |
| 3.1.6 | Odniesienia i normy .....  | 43 |
| 3.1.7 | Kwestie związane z nadzorem .....  | 43 |
| 3.2   | Cele w zakresie bezpieczeństwa i planowanie.....                                 | 44 |
| 3.2.1 | Wymóg regulacyjny.....   | 44 |
| 3.2.2 | Cel.....   | 44 |
| 3.2.3 | Noty wyjaśniające .....  | 44 |
| 3.2.4 | Dowody .....   | 45 |
| 3.2.5 | Przykłady dowodów .....  | 45 |
| 3.2.6 | Kwestie związane z nadzorem .....  | 46 |
| 4     | Wsparcie .....   | 47 |
| 4.1   | Zasoby .....   | 47 |
| 4.1.1 | Wymóg regulacyjny.....   | 47 |
| 4.1.2 | Cel.....   | 47 |
| 4.1.3 | Noty wyjaśniające .....  | 47 |
| 4.1.4 | Dowody .....   | 47 |
| 4.1.5 | Przykłady dowodów .....  | 48 |
| 4.1.6 | Kwestie związane z nadzorem .....  | 48 |
| 4.2   | Kompetencja .....  | 49 |
| 4.2.1 | Wymóg regulacyjny.....   | 49 |
| 4.2.2 | Cel.....   | 49 |
| 4.2.3 | Noty wyjaśniające .....  | 50 |

|       |   |    |
|-------|---|----|
| 4.2.4 | Dowody .....  | 51 |
| 4.2.5 | Przykłady dowodów .....                               | 51 |
| 4.2.6 | Odniesienia i normy .....                             | 53 |
| 4.2.7 | Kwestie związane z nadzorem .....                     | 53 |
| 4.3   | Świadomość .....                                      | 55 |
| 4.3.1 | Wymóg regulacyjny.....                                | 55 |
| 4.3.2 | Cel.....  | 55 |
| 4.3.3 | Noty wyjaśniające .....                               | 55 |
| 4.3.4 | Dowody .....  | 55 |
| 4.3.5 | Przykłady dowodów .....                               | 55 |
| 4.3.6 | Kwestie związane z nadzorem .....                     | 56 |
| 4.4   | Informowanie i komunikowanie .....                    | 57 |
| 4.4.1 | Wymóg regulacyjny.....                                | 57 |
| 4.4.2 | Cel.....  | 57 |
| 4.4.3 | Noty wyjaśniające .....                               | 57 |
| 4.4.4 | Dowody .....  | 58 |
| 4.4.5 | Przykłady dowodów .....                               | 59 |
| 4.4.6 | Kwestie związane z nadzorem .....                     | 60 |
| 4.5   | Dokumentacja .....                                    | 61 |
| 4.5.1 | Wymóg regulacyjny.....                                | 61 |
| 4.5.2 | Cel.....  | 62 |
| 4.5.3 | Noty wyjaśniające .....                               | 62 |
| 4.5.4 | Dowody .....  | 63 |
| 4.5.5 | Przykłady dowodów .....                               | 64 |
| 4.5.6 | Odniesienia i normy .....                             | 65 |
| 4.5.7 | Kwestie związane z nadzorem .....                     | 65 |
| 4.6   | Integracja czynników ludzkich i organizacyjnych ..... | 66 |
| 4.6.1 | Wymóg regulacyjny.....                                | 66 |
| 4.6.2 | Cel.....  | 66 |
| 4.6.3 | Noty wyjaśniające .....                               | 66 |
| 4.6.4 | Dowody .....  | 67 |
| 4.6.5 | Przykłady dowodów .....                               | 67 |
| 4.6.6 | Odniesienia i normy .....                             | 68 |
| 4.6.7 | Kwestie związane z nadzorem .....                     | 69 |
| 5     | Działalność .....                                     | 70 |
| 5.1   | Planowanie operacyjne i kontrola operacyjna.....      | 70 |
| 5.1.1 | Wymóg regulacyjny.....                                | 70 |
| 5.1.2 | Cel.....  | 71 |
| 5.1.3 | Noty wyjaśniające .....                               | 72 |
| 5.1.4 | Dowody .....  | 74 |
| 5.1.5 | Przykłady dowodów .....                               | 75 |
| 5.1.6 | Odniesienia i normy .....                             | 77 |
| 5.1.7 | Kwestie związane z nadzorem .....                     | 77 |
| 5.2   | Zarządzanie składnikami aktywów.....                  | 78 |

|       |  |     |
|-------|--|-----|
| 5.2.1 | Wymóg regulacyjny.....                   | 78  |
| 5.2.2 | Cel.....                                 | 79  |
| 5.2.3 | Noty wyjaśniające .....                  | 79  |
| 5.2.4 | Dowody .....                             | 81  |
| 5.2.5 | Przykłady dowodów .....                  | 83  |
| 5.2.6 | Odniesienia i normy .....                | 88  |
| 5.2.7 | Kwestie związane z nadzorem .....        | 88  |
| 5.3   | Wykonawcy, partnerzy i dostawcy .....    | 89  |
| 5.3.1 | Wymóg regulacyjny.....                   | 89  |
| 5.3.2 | Cel.....                                 | 89  |
| 5.3.3 | Noty wyjaśniające .....                  | 90  |
| 5.3.4 | Dowody .....                             | 90  |
| 5.3.5 | Przykłady dowodów .....                  | 91  |
| 5.3.6 | Kwestie związane z nadzorem .....        | 92  |
| 5.4   | Zarządzanie zmianą.....                  | 93  |
| 5.4.1 | Wymóg regulacyjny.....                   | 93  |
| 5.4.2 | Cel.....                                 | 93  |
| 5.4.3 | Noty wyjaśniające .....                  | 93  |
| 5.4.4 | Dowody .....                             | 93  |
| 5.4.5 | Przykłady dowodów .....                  | 94  |
| 5.4.6 | Kwestie związane z nadzorem .....        | 95  |
| 5.5   | Zarządzanie sytuacjami kryzysowymi ..... | 96  |
| 5.5.1 | Wymóg regulacyjny.....                   | 96  |
| 5.5.2 | Cel.....                                 | 97  |
| 5.5.3 | Noty wyjaśniające .....                  | 97  |
| 5.5.4 | Dowody .....                             | 97  |
| 5.5.5 | Przykłady dowodów .....                  | 98  |
| 5.5.6 | Kwestie związane z nadzorem .....        | 99  |
| 6     | Ocena wyników .....                      | 100 |
| 6.1   | Monitorowanie .....                      | 100 |
| 6.1.1 | Wymóg regulacyjny.....                   | 100 |
| 6.1.2 | Cel.....                                 | 100 |
| 6.1.3 | Noty wyjaśniające .....                  | 100 |
| 6.1.4 | Dowody .....                             | 101 |
| 6.1.5 | Przykłady dowodów .....                  | 101 |
| 6.1.6 | Odniesienia i normy .....                | 102 |
| 6.1.7 | Kwestie związane z nadzorem .....        | 102 |
| 6.2   | Audyt wewnętrzny .....                   | 103 |
| 6.2.1 | Wymóg regulacyjny.....                   | 103 |
| 6.2.2 | Cel.....                                 | 103 |
| 6.2.3 | Noty wyjaśniające .....                  | 103 |
| 6.2.4 | Dowody .....                             | 103 |
| 6.2.5 | Przykłady dowodów .....                  | 104 |
| 6.2.6 | Odniesienia i normy .....                | 104 |



|       |  |     |
|-------|--|-----|
| 6.2.7 | Kwestie związane z nadzorem .....  | 105 |
| 6.3   | Przegląd dokonywany przez kierownictwo.....  | 106 |
| 6.3.1 | Wymóg regulacyjny.....   | 106 |
| 6.3.2 | Cel.....   | 106 |
| 6.3.3 | Dowody .....   | 106 |
| 6.3.4 | Przykłady dowodów .....  | 107 |
| 6.3.5 | Kwestie związane z nadzorem .....  | 107 |
| 7     | Doskonalenie.....  | 109 |
| 7.1   | Wyciąganie wniosków z wypadków i incydentów .....  | 109 |
| 7.1.1 | Wymóg regulacyjny.....   | 109 |
| 7.1.2 | Cel.....   | 109 |
| 7.1.3 | Noty wyjaśniające .....  | 109 |
| 7.1.4 | Dowody .....   | 110 |
| 7.1.5 | Przykłady dowodów .....  | 111 |
| 7.1.6 | Odniesienia i normy .....  | 112 |
| 7.1.7 | Kwestie związane z nadzorem .....  | 113 |
| 7.2   | Ciągłe doskonalenie .....  | 114 |
| 7.2.1 | Wymóg regulacyjny.....   | 114 |
| 7.2.2 | Cel.....   | 114 |
| 7.2.3 | Noty wyjaśniające .....  | 114 |
| 7.2.4 | Dowody .....   | 116 |
| 7.2.5 | Przykłady dowodów .....  | 117 |
| 7.2.6 | Kwestie związane z nadzorem .....  | 118 |
|       | Załącznik 1 – Tabele korelacji .....   | 119 |
|       | Załącznik 2 – Wzajemna akceptacja zezwoleń, uznań lub certyfikatów produktów lub usług<br>wydawana zgodnie z prawem Unii ..... | 127 |
|       | Załącznik 3 – Eksploatacja bocznic, ustalenia umowne i partnerstwa .....   | 132 |
|       | Załącznik 4 – Kultura bezpieczeństwa .....   | 136 |
|       | Załącznik 5 – Czynniki ludzkie i organizacyjne .....   | 142 |
|       | Załącznik 6 – Definicje .....  | 146 |

Usprawnianie funkcjonowania  
systemu kolejowego  
na rzecz społeczeństwa.

## 1 Kontekst organizacji

### 1.1 Wymóg regulacyjny

1.1 Organizacja musi:

- (a) opisać rodzaj, **charakter**, zakres i obszar swojej działalności;
- (b) wskazać poważne ryzyka dla bezpieczeństwa wynikające z jej działalności kolejowej, niezależnie od tego, czy jest ona prowadzona przez samą organizację, czy też przez wykonawców, partnerów lub dostawców będących pod jej kontrolą;
- (c) wskazać zainteresowane strony (np. organy regulacyjne, inne organy, **przewoźników kolejowych**, zarządców infrastruktury, wykonawców, dostawców, partnerów), w tym strony poza systemem kolejowym, które mają znaczenie dla systemu zarządzania bezpieczeństwem;
- (d) wskazać i utrzymać wymogi prawne i inne wymogi związane z bezpieczeństwem pochodzące od zainteresowanych stron, o których mowa w lit. c);
- (e) zapewnić, by wymogi, o których mowa w lit. d), były uwzględniane przy opracowywaniu, wdrażaniu i utrzymaniu systemu zarządzania bezpieczeństwem;
- (f) opisać zakres systemu zarządzania bezpieczeństwem, wskazując, które części działalności są objęte tym zakresem i które nie są nim objęte, przy uwzględnieniu wymogów, o których mowa w lit. d).

1.2 Do celów niniejszego załącznika stosuje się następujące definicje:

- (a) „**charakter**” w odniesieniu do działalności kolejowej prowadzonej przez zarządców infrastruktury oznacza scharakteryzowanie tej działalności poprzez jej zakres, obejmujący projektowanie i budowę infrastruktury, utrzymanie infrastruktury, planowanie ruchu oraz zarządzanie i sterowanie ruchem, oraz poprzez wykorzystanie infrastruktury kolejowej, obejmujące linie konwencjonalne lub linie dużych prędkości oraz przewóz osób lub towarów;
- (b) „**zakres**” w odniesieniu do działalności kolejowej prowadzonej przez zarządców infrastruktury oznacza zakres scharakteryzowany przez długość torów linii kolejowych oraz szacowaną wielkość zarządcy infrastruktury pod względem liczby jego pracowników zatrudnionych w sektorze kolejowym.

### 1.2 Cel

Wnioskodawca powinien z zachowaniem należytej staranności udowodnić władzom, że jego system zarządzania bezpieczeństwem obejmuje całość prowadzonej działalności. Organ dokonujący oceny powinien być w stanie wyraźnie określić charakter działania i sposób zarządzania nim w ramach systemu zarządzania bezpieczeństwem. Wnioskodawca powinien udowodnić, że dokładnie rozumie stosunki łączące go z zainteresowanymi stronami oraz poważne ryzyko, na jakie jest narażony, oraz że wie, kto jest narażony i w jaki sposób rozwiązać te kwestie w ramach systemu zarządzania bezpieczeństwem.

### 1.3 Noty wyjaśniające

W punkcie 1.1 przywołanego powyżej tekstu prawnego w zakresie dotyczącym wymagań odnośnie zarządcy infrastruktury „rodzaj” zamieniony został na „charakter” a „obszar” został usunięty.

„Organizacja” wymogów, ich kontekst i zakres stosowania systemu zarządzania bezpieczeństwem **(1.1)** są ukierunkowane na lepsze zrozumienie działalności organizacji, oczekiwań zainteresowanych stron i środowiska, w jakim funkcjonuje organizacja, z perspektywy podmiotu oceniającego. Charakter organizacji jest punktem wyjścia dla oceny; posiadanie takiej informacji na początku procesu składania wniosku umożliwi wnioskodawcy określenie, czym się zajmuje i jaką strukturę posiada jego organizacja; to z kolei pozwoli podmiotowi oceniającemu podjąć decyzje w sprawie sposobu zaplanowania oceny. Na przykład, jeżeli organizacja jest scentralizowana lub prowadzi różne działania, zapewniając dużą swobodę władzom lokalnym w zakresie planowania i organizowania ich działań, lub jeżeli organizacja zatrudnia więcej lub mniej wykonawców, oczekuje się odpowiednio, że organizacja wnioskodawcy i jego system zarządzania bezpieczeństwem będą posiadały strukturę umożliwiającą rozwiązywanie pojawiających się problemów. Organizacja powinna jasno wyjaśnić, kim są jej wykonawcy, jakiego rodzaju monitoring jest prowadzony (zob. również sekcja 6.1) oraz jak wnioskodawca zarządza odpowiedzialnością za różne aspekty działalności. Powinno być również jasne, gdzie leży odpowiedzialność pomiędzy systemem zarządzania bezpieczeństwem wnioskodawcy a systemem zarządzania bezpieczeństwem każdej innej powiązanej organizacji. W ramach wyjaśnienia ogólnego kontekstu organizacji można również wskazać sposób zarządzania czynnikami ludzkimi i organizacyjnymi. Struktura, którą określono w punkcie 4 ISO High Level Structure, może pomóc zrozumieć prace przygotowawcze niezbędne przed ustanowieniem systemu zarządzania bezpieczeństwem. Niezwykle istotne jest, aby podmiot oceniający znał zakres działalności, jeżeli miałby przeprowadzić odpowiednią ocenę.

Zgodnie z definicją rodzaj działalności **[1.1. lit. a)]** obejmuje przewóz osób (z przewozami dużych prędkości lub bez nich) i towarów (z ładunkami niebezpiecznymi lub bez nich) oraz usługi manewrowe. Może również obejmować inne szczególne rodzaje działalności, takie jak przeprowadzanie testów pojazdów, eksploatacja pojazdów związana z działalnością mającą na celu utrzymanie infrastruktury kolejowej lub eksploatacja pojazdów na prywatnych bocznicach. Bardziej szczegółowe informacje na temat rodzaju, zakresu i obszaru działalności znajdują się w *przewodniku Agencji dotyczącym wniosków o wydanie jednolitych certyfikatów bezpieczeństwa*. Dodatkowe informacje na temat eksploatacji bocznicy znajdują się w części Załącznik 3.

Dla zarządcy infrastruktury „charakter” i „zakres” **(1.2)** oznaczają naturę prowadzonej działalności biznesowej oraz jej zakres geograficzny i złożoność. „Charakter” odnosi się do rodzaju zarządzanej infrastruktury, tego, jak jest nowoczesna, czy jest konwencjonalna, dużych prędkości lub posiada obie te cechy, podczas gdy „zakres” odnosi się do rodzaju prowadzonej działalności.

Identyfikacja poważnych zagrożeń w tym przypadku oznacza, że wnioskodawca powinien wykazać, że dzięki przeprowadzonej analizie ryzyka, na jakie jest narażony, wie, które rodzaje ryzyka są najistotniejsze. Identyfikacja poważnych zagrożeń oznacza również, że wnioskodawca ustanowił system zarządzania ryzykiem (lub przygotowuje się do jego ustanowienia) i dzięki niemu może:

- *analizować niebezpieczne zdarzenia i oceniać czynniki ryzyka,*
- *zdawać sobie sprawę z najistotniejszych kwestii (w zakresie konsekwencji i częstotliwości) oraz*
- *priorytetowo traktować środki ukierunkowane na zapobieganie wypadkom. [1.1. lit. b)]*

Pomoże to w określeniu kontekstu organizacji i uświadomi organowi dokonującemu oceny, że wnioskodawcy rozumieją środowisko, w którym funkcjonują. Działalność innych podmiotów lub stron spoza systemu kolejowego [1.1. lit. c)] może wpływać na bezpieczeństwo działań i w związku z tym należy ją uwzględnić w ocenie ryzyka. Dodatkowe informacje dotyczące ustaleń umownych i partnerstw można znaleźć w części Załącznik 3.

Wnioskodawca powinien również dostarczyć wystarczających informacji, aby jednostka certyfikująca ds. bezpieczeństwa mogła zrozumieć, jakiego rodzaju operacje wykonuje przedsiębiorstwo i gdzie; na przykład,

jakie ładunki przedsiębiorstwo będzie przewozić, tj. drewno, kontenery, transport kombinowany, naczepy w wagonach kieszeniowych, towary w wagonach lub na otwartych wagonach itp., oraz jakie trasy są obsługiwane. W przypadku różnych rodzajów towarów przedsiębiorstwo może potrzebować różnych rodzajów rozwiązań w zakresie zarządzania, o których mowa w systemie zarządzania bezpieczeństwem (załadunek, szkolenie itp.).

W kontekście organizacji należy również opisać, w jaki sposób przedsiębiorstwo kolejowe lub zarządca infrastruktury planuje zająć się utrzymaniem wszystkich pojazdów, z których będzie korzystać. Na przykład czy organizacja będzie korzystać z certyfikowanego podmiotu odpowiedzialnego za utrzymanie, czy też organizacja chce stać się podmiotem odpowiedzialnym za utrzymanie i utrzymywać pojazdy wyłącznie na potrzeby własnej działalności oraz spełniać odpowiednie wymagania dotyczące podmiotów odpowiedzialnych za utrzymanie (zob. załącznik II [rozporządzenia \(UE\) 2019/779](#) i związany z nim Przewodnik), w obrębie systemu zarządzania bezpieczeństwem. Wnioskodawca musi określić relacje między różnymi kontrahentami w zakresie utrzymania, na przykład jeśli przedsiębiorstwo kolejowe wynajmuje pojazdy, które są utrzymywane przez zewnętrzny podmiot odpowiedzialny za utrzymanie, należy to określić. Dalsze informacje na temat zarządzania działaniami w zakresie utrzymania można znaleźć w przewodniku ERA dotyczącym podmiotów odpowiedzialnych za utrzymanie.

Identyfikacja obowiązujących wymogów związanych z bezpieczeństwem **[1.1. lit. d)]** obejmuje przepisy obowiązujących rozporządzeń UE (np. odpowiednie CSM dotyczące systemów zarządzania bezpieczeństwem, w szczególności załącznik I i załącznik II do nich, wspólną metodę oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka, wspólną metodę oceny bezpieczeństwa w odniesieniu do monitorowania, odpowiednie TSI, akt wykonawczy dotyczący praktycznych ustaleń w zakresie certyfikacji bezpieczeństwa oraz, w stosownych przypadkach, akt wykonawczy w sprawie praktycznych ustaleń dotyczących zezwolenia na wprowadzenie pojazdu do obrotu oraz rozporządzenie w sprawie podmiotów odpowiedzialnych za utrzymanie) i przepisy krajowe (np. zgłoszone przepisy krajowe, prawo krajowe) oraz wszelkie inne wymagania, którym podlega organizacja (np. sektorowe lub branżowe zasady dotyczące ruchu pociągów lub normy dotyczące systemu zarządzania i normy techniczne, takie jak ISO, CEN/CENELEC, UIC).

W tej sekcji organizacja identyfikuje wymagania prawne, które musi spełnić, oraz normy stosowane w sektorze i inne normy, których stosowanie warunkuje bezpieczne prowadzenie ruchu pociągów. W różnych państwach członkowskich mogą obowiązywać różne wymagania, a system zarządzania bezpieczeństwem musi umożliwiać zarządzanie wszelkimi konfliktami między nimi a ramami prawnymi. Dalsze informacje związane z tymi wymogami można znaleźć w dokumentach, takich jak regulamin sieci.

Jeżeli przedsiębiorstwo kolejowe planuje transport towarów niebezpiecznych lub zarządca infrastruktury planuje zezwolić na transport towarów niebezpiecznych w swojej infrastrukturze, obaj muszą spełnić szczegółowe wymagania określone w regulaminie dla międzynarodowego przewozu kolejami towarów niebezpiecznych (RID), jak również wszelkich obowiązujących przepisach krajowych. Regulamin RID zawiera szczególne wymagania dotyczące szkolenia personelu zaangażowanego w transport towarów niebezpiecznych, takiego jak doradca ds. bezpieczeństwa, jak również na przykład wymagania dotyczące planów awaryjnych, i powinny one być uwzględnione w systemie zarządzania bezpieczeństwem (zob. również UIC – IRS 40471-3).

Do celów niniejszego dokumentu termin „personel”, „zatrudnieni” i „pracownicy” ma takie samo znaczenie i odnosi się do ludzi pracujących pod bezpośrednią kontrolą organizacji wnioskodawcy.

#### 1.4 Dowody

- *W przypadku przedsiębiorstw kolejowych: informacje na temat charakteru działalności, np. transport pasażerski lub towarowy, przewóz towarów niebezpiecznych, zasięg geograficzny (przez uwzględnienie mapy lub planu trasy) oraz wielkość operacji, korzystanie z podwykonawców, partnerstwo z innymi operatorami (nazwa), różne zaangażowane podmioty (nazwa i rodzaj podmiotu), wybór certyfikowanego podmiotu odpowiedzialnego za utrzymanie wraz z kopią ważnego*

certyfikatu. Należy również określić rodzaje taboru, liczbę bezpośrednio zatrudnionych pracowników oraz wskazanie, skąd zatrudniani są dodatkowi pracownicy, a w przypadku gdy wniosek dotyczy odnowienia świadectwa, wszelkie zmiany dokonane od czasu ostatniej oceny; **[1.1 lit. a)]**

- w przypadku zarządców infrastruktury: informacje na temat charakteru prowadzonej działalności, np. przewóz towarów lub pasażerów, manewrowanie lub inne usługi w zakresie infrastruktury (o których mowa w załączniku II do dyrektywy 2012/34/UE) mające wpływ na bezpieczeństwo kolei, zasięgu geograficznego (przez uwzględnienie map lub planów trasy) oraz skali działalności przedsiębiorstw kolejowych prowadzonej w ramach sieci. Zarządca infrastruktury powinien również uwzględnić informacje dotyczące korzystania z usług podwykonawców (nazwa), partnerstw z innymi operatorami (nazwa), różnych zaangażowanych podmiotów (nazwa i rodzaj), wyboru certyfikowanego podmiotu odpowiedzialnego za utrzymanie wraz z kopią ważnego certyfikatu. Powinien również wskazać informacje dotyczące każdego taboru kolejowego (w tym maszyn służących do utrzymania infrastruktury lub jej pomiarów), jaki może poruszać się po zarządzanej infrastrukturze, oraz powinien wskazać liczbę zatrudnianych pracowników, jak również w przypadku przedłużenia wszelkie zmiany w zakresie zatrudnienia od momentu ostatniej oceny; **[1.1 lit. a)]**
- wnioskodawca ma obowiązek wskazać, jakie są najpoważniejsze zagrożenia dla bezpieczeństwa wpływające na jego działalność; **[1.1. lit. b)]**
- wnioskodawca ubiegający się o certyfikat bezpieczeństwa lub autoryzację bezpieczeństwa musi wykazać, w jaki sposób określił odpowiednie wymogi prawne, np. wymogi oceny CSM, techniczne specyfikacje interoperacyjności, w szczególności te związane z podsystemem „Ruch kolejowy” (TSI OPE), obowiązujące przepisy krajowe oraz inne wymogi (zasady sektorowe, inne zasady), których będzie musiał przestrzegać, aby w bezpieczny sposób prowadzić pociągi, a także musi wykazać, w jaki sposób utrzymuje zgodność z tymi wymogami (procesy w ramach systemu zarządzania bezpieczeństwem wspierające zgodność; **[1.1. lit. c)–d)]**
- wnioskodawca ma obowiązek określić zainteresowane strony mające znaczenie dla pomyślnego wdrożenia systemu zarządzania bezpieczeństwem (których działania mają rzeczywisty lub potencjalny wpływ na system zarządzania bezpieczeństwem, np. kontrahenci, partnerzy), ze wskazaniem, dlaczego są one potrzebne dla poprawnego funkcjonowania systemu zarządzania bezpieczeństwem; **[1.1 lit. c)–d)]**
- w przypadku obu: wnioskodawca powinien wskazać, gdzie w dokumentacji dotyczącej jego systemu zarządzania bezpieczeństwem można znaleźć wszystkie wymogi dotyczące systemu zarządzania bezpieczeństwem, w tym wymogi dotyczące obowiązujących technicznych specyfikacji interoperacyjności, w szczególności TSI OPE, oraz odpowiednie zgłoszone przepisy krajowe i inne wymogi; **[1.1. lit. e)]**
- wnioskodawca musi dostarczyć informacje dotyczące zakresu stosowania systemu zarządzania bezpieczeństwem (w tym musi wyznaczyć granice w odniesieniu do innych części działalności, takich jak utrzymanie pojazdów) **[1.1. lit. f)]**.

## 1.5 Przykłady dowodów

Mapa przedstawiająca geograficzny obszar działalności. Informacje dotyczące taboru kolejowego dopuszczonego do eksploatacji (w tym, w stosownych przypadkach, informacje dotyczące każdego taboru kolejowego proponowanego do eksploatacji w okresie ważności certyfikatu lub autoryzacji oraz informacje dotyczące wszelkich ograniczeń nałożonych na obszar użytkowania). Należy uwzględnić informacje dotyczące rodzajów usług, jakie dany podmiot zamierza świadczyć (przewóz pasażerów lub towarów).

Jeżeli wnioskodawca jest zarządcą infrastruktury, informacje te można przedstawić przez odniesienie np. do:

- informacji zawartych w rejestrze infrastruktury (RINF) opracowanym zgodnie z [dyrektywą \(UE\) 2016/797](#) (art. 49);

- treści regulaminu sieci (w szczególności w sekcji I) opracowanego zgodnie z [dyrektywą 2012/34/UE](#); oraz
- opisu tras opracowanego zgodnie z [rozporządzeniem \(UE\) 2019/773 \(TSI OPE\)](#).

Informacje dostarczone, aby uzyskać autoryzację bezpieczeństwa lub certyfikat bezpieczeństwa, powinny być odpowiednio udokumentowane w celu udowodnienia zgodności z prawem Unii.

Wskazanie obecnego i proponowanego poziomu zatrudnienia w okresie ważności jednolitego certyfikatu bezpieczeństwa, o ile jest on znany.

Przedsiębiorstwo kolejowe dostarcza informacje dotyczące swoich powiązań organizacyjnych, w tym z zarządcami infrastruktury, innymi przedsiębiorstwami kolejowymi, wykonawcami i służbami ratowniczymi. Informacje te powinny zawierać wszelkie specyficzne wymagania zarządcy infrastruktury, które mogą wpłynąć na system zarządzania bezpieczeństwem przedsiębiorstwa kolejowego.

W przypadku przedsiębiorstw kolejowych tabela orientacyjna przedstawiona za pośrednictwem punktu kompleksowej obsługi (OSS) jako część dokumentacji wniosku o wydanie certyfikatu bezpieczeństwa może posłużyć wyjaśnieniu zgodności z przepisami prawnymi i innymi istotnymi wymaganiami.

Podobnie zarządca infrastruktury powinien dostarczyć podobny wykaz podmiotów, takich jak przedsiębiorstwa kolejowe korzystające z kontrolowanej infrastruktury, wykonawcy, sąsiadujący zarządcy infrastruktury, place budowy, władze lokalne (w przypadku powiązań w transporcie drogowym) i służby ratownicze, z którymi łączą go powiązania organizacyjne.

Informacje dotyczące przepisów prawnych (zarówno krajowych, jak i europejskich), których podmiot będzie przestrzegał.

Opis (obejmujący schemat organizacyjny), w ramach którego określa się strukturę systemu zarządzania bezpieczeństwem i sposób zarządzania nim w ramach organizacji, zawiera również powiązania z różnymi sekcjami systemu zarządzania bezpieczeństwem, w których można znaleźć bardziej szczegółowe informacje, takie jak zasady funkcjonowania.

Aktualna kopia rocznego sprawozdania, w którym wyszczególnione są najbardziej istotne ryzyka, z jakimi zmagają się organizacja, oraz uwzględnienie ich w celach bezpieczeństwa, metody stosowane do ich oceny oraz sposób określenia ich priorytetu.

Oświadczenie, czy korzysta się z usług certyfikowanego podmiotu odpowiedzialnego za utrzymanie, czy utrzymuje się pojazdy wyłącznie na potrzeby własnej działalności.

Przegląd procesu utrzymania oraz rodzaj i poziom przeprowadzanych czynności.

Uwzględnienie czynników ludzkich i organizacyjnych oraz poprawa kultury bezpieczeństwa będą miały pozytywny wpływ na spełnienie odpowiedniego wymogu systemu zarządzania bezpieczeństwem, a dowody na to można znaleźć w następujących źródłach:

Rejestr zagrożeń lub przegląd, w których dokumentowano scenariusze operacyjnego ryzyka dla bezpieczeństwa, z uwzględnieniem czynników ludzkich i organizacyjnych:

- osób fizycznych (np. błąd ludzki);
- miejsca pracy (np. środowisko fizyczne, jak hałas, ciemność, pogoda); oraz
- organizacji (np. obciążenie pracą, zarządzanie kompetencjami, projektowanie zadań, zasoby, zmiany).

Przy określaniu najpoważniejszych zagrożeń ocenia się scenariusze ryzyka, aby umożliwić ustalenie priorytetów ryzyka (można to znaleźć w procesie oceny ryzyka, zob. sekcja 3.1.1). Rejestr zagrożeń obejmuje zagrożenia związane z działalnością organizacji, a także działaniami realizowanymi przez kontrahentów, partnerów lub dostawców pozostających pod jej kontrolą. W przypadku każdego poważnego zagrożenia jego właściciel jest wyraźnie zdefiniowany w ramach systemu zarządzania bezpieczeństwem.

System zarządzania bezpieczeństwem zawiera opis zainteresowanych stron, które mają znaczenie dla zarządzania bezpieczeństwem oraz opisuje sposób zarządzania relacjami z tymi zainteresowanymi stronami. Wskazano sposoby informowania zainteresowanych osób trzecich o najpoważniejszych zagrożeniach i podano kilka przykładów (np. umowy, protokoły z posiedzeń).

## 1.6 Odniesienia i normy

- [Przewodnik dotyczący wniosków w zakresie TSI OPE](#)
- [Wytyczne dotyczące podmiotów odpowiedzialnych za utrzymanie](#)
- [Inspekcje przesyłek towarów niebezpiecznych UIC - IRS 40471-3](#)

## 1.7 Kwestie związane z nadzorem

Należy sprawdzić dokładność dostarczonych informacji w porównaniu ze znanymi informacjami na temat bieżących działań w przypadku wniosku o odnowienie certyfikatu lub w porównaniu z innymi dostępnymi informacjami w przypadku nowego operatora.

Należy sprawdzić, czy w ramach systemu zarządzania bezpieczeństwem – zgodnie z opisem – realizowane są ustalenia dotyczące bezpiecznego zarządzania w praktyce.

Należy sprawdzić, czy wszystkie powiązania organizacji z innymi podmiotami są odzwierciedlone w ustaleniach w ramach systemu zarządzania bezpieczeństwem w celu kontrolowania ryzyka.

## 2 Przywództwo

### 2.1 Przywództwo i zaangażowanie

#### 2.1.1 Wymóg regulacyjny

2.1.1. Kadra kierownicza wyższego szczebla musi wykazać się przywództwem oraz zaangażowaniem w opracowanie, wdrożenie, utrzymanie i ciągłe doskonalenie systemu zarządzania bezpieczeństwem poprzez:

- (a) przejęcie ogólnej rozliczalności i odpowiedzialności za bezpieczeństwo;
- (b) zapewnienie zaangażowania na rzecz bezpieczeństwa ze strony kierownictwa różnych szczebli w obrębie organizacji poprzez jego działania oraz w jego stosunkach z pracownikami i wykonawcami;
- (c) zapewnienie, by ustanowione zostały polityka w zakresie bezpieczeństwa i cele w zakresie bezpieczeństwa oraz aby ta polityka i te cele zostały zrozumiane oraz były zgodne ze strategicznym ukierunkowaniem organizacji;
- (d) zapewnienie zintegrowania wymogów dotyczących systemu zarządzania bezpieczeństwem z procesami biznesowymi organizacji;
- (e) zapewnienie dostępności zasobów niezbędnych dla systemu zarządzania bezpieczeństwem;
- (f) zapewnienie skuteczności systemu zarządzania bezpieczeństwem w kontrolowaniu ryzyk dla bezpieczeństwa stwarzanych przez organizację;
- (g) zachęcanie pracowników do wspierania działań na rzecz zapewnienia zgodności z wymogami dotyczącymi systemu zarządzania bezpieczeństwem;
- (h) promowanie ciągłego doskonalenia systemu zarządzania bezpieczeństwem;
- (i) zapewnienie, by bezpieczeństwo było uwzględniane przy identyfikacji ryzyk biznesowych organizacji i zarządzaniu tymi ryzykami oraz wyjaśnienie, w jaki sposób rozpoznawane i rozwiązywane będą konflikty między bezpieczeństwem a innymi celami biznesowymi;
- (j) promowanie pozytywnej kultury bezpieczeństwa.

#### 2.1.2 Cel

Określenie jasnego i właściwego kierunku zarządzania bezpieczeństwem będzie miało istotny wpływ na sposób zarządzania ryzykiem. Organ dokonujący oceny musi być pewny, że wnioskodawca zobowiązał się przekazać środki, aby umożliwić bezpieczne funkcjonowanie organizacji i skuteczne zarządzanie ryzykiem, a także musi mieć pewność, że przywództwo w organizacji wnioskodawcy zapewnia osiągnięcie tych celów. Zaangażowanie ze strony kierownictwa w zakresie czynników ludzkich i organizacyjnych odzwierciedlono w politykach i celach oraz w zachowaniach związanych z zarządzaniem i przywództwem. Ponadto podejście oparte na czynnikach ludzkich i organizacyjnych przyjęte przez kierownictwo również zagwarantuje, aby proces opracowywania szkoleń i procedur opierał się na zadaniach wykonywanych w naturalnym otoczeniu, co pomoże zoptymalizować zarówno kontrolę ryzyka, jak i wydajność, ponieważ będzie oparty na dokładnym opisie zadania („faktyczne funkcjonowanie”).

Strategia w zakresie bezpieczeństwa określa znaczenie i priorytetyzację bezpieczeństwa, uwzględniając integrację czynników ludzkich i organizacyjnych oraz promowanie kultury bezpieczeństwa.

Organizacja sprzyja zachowaniu ciągłej i zbiorowej czujności, walce z samozadowoleniem („wszystko jest pod kontrolą”) i nadmiernym upraszczaniem („przestrzeganie procedur wystarczy, aby zachować bezpieczeństwo”) oraz rozwojowi postaw w zakresie kwestionowania. Ponadto wszystkie podmioty w



organizacji mają świadomość, że, niezależnie od jakości planowania i organizacji, barier i procedur technicznych, zawsze może istnieć rozbieżność między oczekiwaniami i rzeczywistością. Do wykrywania i wspólnego analizowania tych sytuacji, które nie zostały odpowiednio przewidziane, wykorzystuje się wszystkie możliwe źródła.

Ponadto komunikat organizacji dotyczący bezpieczeństwa jest zgodny ze stanem rzeczywistym decyzji kierownictwa.

W celu zapewnienia właściwego funkcjonowania i doskonalenia systemu zarządzania bezpieczeństwem zasadnicze jest, aby kierownictwo wykazywało w stosunkach z personelem i zainteresowanymi stronami, że wyznacza pozytywny kierunek w zarządzaniu bezpieczeństwem. Osoby na kierowniczych stanowiskach mają największy wpływ na kulturę organizacji i dlatego kluczowe jest, aby przekazywały właściwe sygnały osobom pozostającym pod ich zwierzchnością. Zachowanie osób zarządzających na wszystkich szczeblach organizacji i waga, jaką przykładają oni do bezpieczeństwa w codziennych decyzjach, wpływa w istotny sposób na zachowanie innych podmiotów w wypełnianiu ich zadań w bezpieczny sposób. Ponadto kadra zarządzająca powinna stworzyć fizyczne i społeczne środowisko pracy, w którym praca na stanowiska wykonawczych jest wykonywana bezpiecznie.

### 2.1.3 Noty wyjaśniające

„Kadra kierownicza wyższego szczebla” (**2.1.1**) w tym kontekście oznacza tych, którzy podejmują decyzje jako kierownictwo organizacji. Zazwyczaj będzie to dyrektor generalny, członkowie kadry kierowniczej wyższego szczebla, przewodniczący i członkowie zarządu. Od „kadry kierowniczej wyższego szczebla”, zarówno jako od grupy, jak i od osób, wymaga się wykazania się przywództwem i zaangażowaniem w systemie zarządzania bezpieczeństwem.

#### ***Jak uwzględnić czynniki ludzkie i organizacyjne oraz kulturę bezpieczeństwa?***

Dostateczną wagę należy przywiązywać do ryzyk dla bezpieczeństwa [**2.1.1 lit. i**] w celu zrównoważenia innych ryzyk biznesowych, aby uniknąć sytuacji, w której kadra kierownicza traktuje priorytetowo potrzeby biznesowe w sposób osłabiający skuteczność działania w zakresie bezpieczeństwa. Kadra kierownicza wyższego szczebla musi zapewnić, by do celów odnoszono się w sposób utrzymujący skuteczność działania w zakresie bezpieczeństwa, a ryzykiem zarządzano w zakresie, w jakim jest to praktycznie wykonalne. Sprzeczne cele nie powinny skutkować sprzecznymi zadaniami dla pracowników, co mogłoby prowadzić do problemów związanych z bezpieczeństwem.

Podejście oparte na zintegrowanych czynnikach ludzkich i organizacyjnych w zakresie przywództwa i zarządzania oznacza ustalanie celów, oczekiwań i rozliczalności w odniesieniu do zachowań związanych z bezpieczeństwem na wszystkich poziomach organizacji oraz zapewnienie terminowej informacji zwrotnej i komunikacji.

### 2.1.4 Dowody

- *Istnieją strategia i cele w zakresie bezpieczeństwa oraz dowody na to, że są one dostępne i zrozumiałe dla wszystkich pracowników oraz wyjaśniono, w jaki sposób wpisują się one w inne procesy gospodarcze i są powiązane z ciągłym doskonaleniem; [**2.1.1 lit. a), b), g), e), h**]*
- *strategia w zakresie bezpieczeństwa określa znaczenie stosowania podejścia opartego na czynnikach ludzkich i organizacyjnych we wszystkich procesach związanych z bezpieczeństwem w celu osiągnięcia wysokiego poziomu bezpieczeństwa w organizacji. Organizacja wykazuje, jak kwestie*

związane z czynnikami ludzkimi i organizacyjnymi są zarządzane w procesach organizacyjnych; **[2.1.1 lit. c)]**

- związek między systemem zarządzania bezpieczeństwem a inną działalnością gospodarczą jest jasno określony w procedurze lub schemacie organizacyjnym; **[2.1.1 lit. e), i)]**
- w strategii w zakresie bezpieczeństwa lub w innych procesach dostępne są informacje wskazujące, że kadra kierownicza zobowiązuje się do zapewnienia i utrzymania wystarczających zasobów, aby umożliwić skuteczne funkcjonowanie i z czasem również poprawę systemu zarządzania bezpieczeństwem; **[2.1.1 lit. e), h)]**
- istnieją dowody na to, że kadra kierownicza promuje pozytywną kulturę bezpieczeństwa; **[2.1.1 lit. j), h)]**
- dowody pokazujące, w jaki sposób zapewnia się zrozumienie ról i obowiązków związanych z bezpieczeństwem przez pracowników oraz w jaki sposób ich działania wpływają na zdolność organizacji do kontrolowania ryzyka za pośrednictwem systemu zarządzania bezpieczeństwem; **[2.1.1 lit. d), f), i)]s**
- w strategii w zakresie bezpieczeństwa lub innej dokumentacji istnieją dowody, że organizacja stara się informować swoich pracowników o istotnej roli, jaką odgrywają w zapewnieniu funkcjonowania systemu zarządzania bezpieczeństwem w praktyce w celu znaczącej kontroli ryzyka; **[2.1.1 lit. e)]**
- istnieją procesy określające, w jaki sposób w organizacji należy uwzględnić i komunikować czynniki ludzkie i organizacyjne związane z celami biznesowymi organizacji i procesami organizacyjnymi, np. projekty, dochodzenia dotyczące incydentów i wypadków, analizy ryzyka i inne działania związane z bezpieczeństwem dla pracowników, wykonawców, partnerów i dostawców organizacji; **[2.2.1 lit. c), d), e)]**
- istnieją dowody wykazujące, że kierownictwo wdrożyło procesy, które zapewnią, że czynniki ludzkie i organizacyjne są w należyty sposób uwzględnione przez podwykonawców organizacji. **[2.2.1 lit. c), d), e)]**

#### 2.1.5 Przykłady dowodów

Strategia w zakresie bezpieczeństwa jest podpisana i opatrzona datą przez dyrektora generalnego i jasno określa zaangażowanie kadry kierowniczej w bezpieczeństwo i poprawę bezpieczeństwa oraz udział personelu w zarządzaniu zagrożeniem dla bezpieczeństwa. Strategia w zakresie bezpieczeństwa określa także sposób jej przeglądu.

Uwzględnienie czynników ludzkich i organizacyjnych oraz poprawa kultury bezpieczeństwa będą miały pozytywny wpływ na spełnienie odpowiedniego wymogu systemu zarządzania bezpieczeństwem, a dowody na to można znaleźć w następujących źródłach:

Jasny zestaw celów w zakresie bezpieczeństwa ustalonych dla organizacji, które są skonkretyzowane, mierzalne, osiągalne, realne i terminowe (SMART), oraz jasna metodyka określona w procedurze ich tworzenia i analizowania powodzenia lub niepowodzenia w ich osiągnięciu. System zarządzania bezpieczeństwem zawiera dowody, że kadra kierownicza ma cele związane z bezpieczeństwem operacyjnym (poza celami związanymi z bezpieczeństwem i higieną pracy).

Jasna deklaracja kadry kierowniczej dotycząca tego, w jaki sposób będzie promowana pozytywna kultura bezpieczeństwa, w tym w jaki sposób personel uczestniczy w tym procesie i jest w niego zaangażowany.

Przegląd spotkań i ich częstotliwości, którego dokonuje kadra kierownicza wyższego szczebla, gdzie bezpieczeństwo jest standardowym elementem sprawozdawczym.

Jasna deklaracja dotycząca zaangażowania organizacji w zapewnienie wystarczających zasobów, aby umożliwić skuteczne funkcjonowanie systemu zarządzania bezpieczeństwem w celu kontroli ryzyka.

Schemat organizacyjny jasno określający sposób funkcjonowania systemu zarządzania bezpieczeństwem i obowiązki poszczególnych osób.

Fakt, że przy projektowaniu nowego sprzętu, np. nowych pociągów, przyjmuje się podejście oparte na czynnikach ludzkich i organizacyjnych. Obejmuje to korzystanie z doświadczenia obecnych użytkowników w zakresie tworzenia wymagań projektowych, analizowanie zadań w celu rozpoznania wyzwań poznawczych i fizjologicznych, zmniejszanie możliwości błędnego działania poprzez projektowanie z zastosowaniem wytycznych dotyczących czynników ludzkich, takich jak międzynarodowe normy, przeprowadzenie analizy zarządzania obciążeniem pracą i zmęczeniem w celu zapewnienia zdolności personelu do wykonywania zadań, dokonywanie analiz ryzyka w celu zidentyfikowania potencjalnych problemów i określenie działań łagodzących w ich zakresie. Uwzględnia się czynniki środowiskowe, takie jak śnieg, ciepło, deszcz itp., a także czynniki społeczno-gospodarcze, takie jak priorytety organizacyjne, zamówienia i kultura narodowa.

Szkolenie w zakresie bezpieczeństwa dla kadry kierowniczej organizowane dla kierowników zajmujących stanowiska związane z bezpieczeństwem. Istnieją dowody na przeprowadzanie okresowych szkoleń dla kadry kierowniczej. Istnieją dowody na to, że szkolenia dla kadry kierowniczej uwzględniają wizję bezpieczeństwa, sposób jej włączenia do strategii w zakresie bezpieczeństwa, a także sposób jej przekazywania i stosowania.

Kierownictwo demonstrujące swoje zobowiązanie do promowania pozytywnej kultury bezpieczeństwa i dawania odpowiedniego przykładu w tym zakresie poprzez kontrole bezpieczeństwa lub wizyty „w terenie”.

#### 2.1.6 Odniesienia i normy

- [Kultura bezpieczeństwa](#) (strona internetowa ERA)

#### 2.1.7 Kwestie związane z nadzorem

Zakres rozbieżności między polityką i procedurami przedstawionymi w powyższych dowodach a rzeczywistością obserwowaną podczas nadzoru i stopień, w jakim organizacja jest świadoma tej luki, to kluczowe kwestie wymagające nadzoru.

W ramach nadzoru należy sprawdzić zakres prawdziwego zaangażowania kadry kierowniczej w promowanie systemu zarządzania bezpieczeństwem i kultury bezpieczeństwa, jak również zaangażowanie pracowników w organizację, poprzez zbadanie własnych mechanizmów organizacji służących zrozumieniu i rozwojowi tej kultury i systemu zarządzania bezpieczeństwem.

Sprawdzenie, czy organizacja może wykazać, że zapewnia wystarczające zasoby na rozwój, wdrożenie, utrzymanie i stałą poprawę systemu zarządzania bezpieczeństwem.

Sprawdzenie, poprzez rozmowy z kadrą kierowniczą wyższego szczebla i innymi pracownikami, w jaki sposób kierownictwo wyraża swoje zaangażowanie w poprawę bezpieczeństwa. Sprawdzenie, jak często i w jaki sposób kontaktuje się z pracownikami w kwestiach bezpieczeństwa lub promowania kultury bezpieczeństwa (warsztaty, fora, specjalne dni bezpieczeństwa itp.).

Sprawdzenie, czy kadra kierownicza wyższego szczebla powiadamia o celach, aby zachęcić wszystkich pracowników do udziału w ich osiągnięciu lub podziękować wszystkim za poprawę skuteczności działania.

## 2.2 Strategia w zakresie bezpieczeństwa

### 2.2.1 Wymóg regulacyjny

|   |
|---|
| <p>2.2.1. Dokument opisujący politykę organizacji w zakresie bezpieczeństwa jest formułowany na poziomie kadry kierowniczej wyższego szczebla i jest:</p> <ul style="list-style-type: none"><li>(a) odpowiedni do rodzaju, <b>charakteru</b> organizacji i zakresu działalności kolejowej;</li><li>(b) zatwierdzony przez dyrektora generalnego organizacji (lub przedstawiciela bądź przedstawicieli kadry kierowniczej wyższego szczebla);</li><li>(c) aktywnie wdrażany, komunikowany i udostępniany wszystkim pracownikom.</li></ul> <p>2.2.2. Polityka w zakresie bezpieczeństwa musi:</p> <ul style="list-style-type: none"><li>(a) zawierać zobowiązanie do spełnienia wszystkich wymogów prawnych i innych wymogów dotyczących bezpieczeństwa;</li><li>(b) zapewniać ramy na potrzeby określania celów w zakresie bezpieczeństwa oraz oceny wyników organizacji w zakresie bezpieczeństwa względem tych celów;</li><li>(c) zawierać zobowiązanie do kontrolowania ryzyk dla bezpieczeństwa będących wynikiem zarówno własnych działań, jak i działań innych podmiotów;</li><li>(d) zawierać zobowiązanie do ciągłego doskonalenia systemu zarządzania bezpieczeństwem;</li><li>(e) być utrzymywana zgodnie ze strategią biznesową oraz oceną wyników organizacji w zakresie bezpieczeństwa.</li></ul> |
|---|

### 2.2.2 Cel

Strategia w zakresie bezpieczeństwa jest ważnym dokumentem pokazującym, w jaki sposób organizacja zarządza swoimi obowiązkami dotyczącymi bezpieczeństwa oraz swoim przywództwem i zaangażowaniem na rzecz właściwego zarządzania bezpieczeństwem. Wnioskodawca powinien być w stanie wykazać, że posiada strategię w zakresie bezpieczeństwa, która spełnia powyższe wymogi i opisuje w skrócie podstawową strukturę kontroli ryzyka.

### 2.2.3 Noty wyjaśniające

Strategia w zakresie bezpieczeństwa jest wyrazem filozofii kadry kierowniczej i dlatego ta sekcja jest ściśle powiązana z sekcją 3.1.

W punkcie 2.2.1 lit. a) przepisu znajdującego się powyżej, w miejscu, gdzie wymagania dotyczą zarządcy infrastruktury, „rodzaj” zastępuje się „charakterem”.

#### **Jak uwzględnić czynniki ludzkie i organizacyjne oraz kulturę bezpieczeństwa?**

Strategia w zakresie bezpieczeństwa zawiera wizję bezpieczeństwa, iż nawet jeśli powyższy wymóg regulacyjny nie odnosi się bezpośrednio do czynników ludzkich i organizacyjnych, istnieje wyraźny nacisk na kwestie związane z czynnikami ludzkimi w organizacji oraz uznanie ważnej roli, jaką ludzie odgrywają w tworzeniu bezpiecznej i wydajnej organizacji oraz realizacji celów biznesowych. Rola człowieka jest rozważana przy każdym przeglądzie rozwoju operacyjnego i biznesowego.

#### 2.2.4 Dowody

- *W przypadku przedsiębiorstwa kolejowego: pisemna strategia w zakresie bezpieczeństwa podpisana przez dyrektora generalnego, która odzwierciedla rodzaj i zakres działalności, wspiera zgodność z wymogami legislacyjnymi i innymi wymogami, ciągłą poprawę bezpieczeństwa i zapewnia ramy na potrzeby określania celów w zakresie bezpieczeństwa. [2.2.1 lit. a), b)], [2.2.2 lit. a)–c)]*
- *W przypadku zarządcy infrastruktury: pisemna strategia w zakresie bezpieczeństwa podpisana przez dyrektora generalnego, która odzwierciedla charakter i zakres działalności kolejowej i rozwoju infrastruktury, wspiera zgodność z wymogami legislacyjnymi i innymi wymogami, ciągłą poprawę bezpieczeństwa i służy do ustalania celów w zakresie bezpieczeństwa; [2.2.2 lit. a)–c)]*
- *W przypadku obu: informacja wskazująca, że o strategii w zakresie bezpieczeństwa poinformowano wszystkich pracowników; [2.2.1 lit. c)]*
- *informacja, że strategia w zakresie bezpieczeństwa jest utrzymywana tak, aby była zawsze zgodna ze strategią biznesową i oceną wyników organizacji w zakresie bezpieczeństwa; [2.2.2 lit. d), e)]*
- *dowody, że strategia w zakresie bezpieczeństwa zawiera zobowiązanie do monitorowania skuteczności działań oraz że jest ona okresowo aktualizowana, po dokonaniu analizy poziomu bezpieczeństwa oraz zmieniana po dokonaniu przeglądu skuteczności działania organizacji w zakresie bezpieczeństwa w odniesieniu do wyznaczonych celów. [2.2.2 lit. b), d), e)]*

#### 2.2.5 Przykłady dowodów

Strategia w zakresie bezpieczeństwa podpisana przez dyrektora naczelnego organizacji i opatrzona datą, która dokładnie odzwierciedla rodzaj, zakres i charakter działalności. Dokument zawiera zobowiązanie do ciągłego doskonalenia systemu zarządzania bezpieczeństwem.

Strategia w zakresie bezpieczeństwa jest aktualna i ma określony cykl przeglądu zgodny ze strategią biznesową.

Strategia w zakresie bezpieczeństwa zawierająca informacje lub odniesienia, w których określono proces jej przeglądu. Ma to na celu określenie konieczności jej zmiany, w wyniku monitorowania wyników działalności organizacji w zakresie bezpieczeństwa w stosunku do ustalonych celów.

Strategia w zakresie bezpieczeństwa i inne powiązane strategie stosowane jako narzędzie ogniskowania działań kierownictwa, w wyniku czego są one interpretowane w ten sam sposób przez wszystkich pracowników.

Pracownicy aktywnie uczestniczący w weryfikacji i zmianach strategii w zakresie bezpieczeństwa i sposobu jej realizacji.

Strategia w zakresie bezpieczeństwa odnosząca się do procesu/metodyki oceny proponowanych decyzji w oparciu o analizę ryzyka (zgodnie z wizją dotyczącą bezpieczeństwa). Proces ten wyjaśnia, w jaki sposób bezpieczeństwo jest brane pod uwagę jako główny cel.

Strategia w zakresie bezpieczeństwa lub inne zapisy w systemie zarządzania bezpieczeństwem upoważniające każdego pracownika do przerwania pracy, gdy warunki pracy stają się niebezpieczne.

Przeprowadzenie podstawowej oceny organizacji w zakresie kultury bezpieczeństwa. Organizacja zidentyfikowała słabe punkty, poinformowała o nich pracowników, a środki poprawy zostały określone w strategii w zakresie bezpieczeństwa.

Istnieje proces powiadamiania o strategii w zakresie bezpieczeństwa za pośrednictwem intranetu organizacji i prezentowania jej w strategicznych/operacyjnych miejscach.

Organizacja jest otwarta, szuka zewnętrznych możliwości uczenia się, aby zwiększyć swoją efektywność i skuteczność, oraz dostrzega w tych działaniach kwestie związane z czynnikiem ludzkim.

### 2.2.6 *Kwestie związane z nadzorem*

Podczas nadzoru ważne będzie sprawdzenie, jak dobrze powiadomiono o strategii w zakresie bezpieczeństwa i jak dobrze rozumieją ją wszyscy pracownicy oraz jaką rolę odgrywa w rzeczywistości przy ustalaniu ram bezpieczeństwa, w których działa organizacja. Kluczową kwestią jest to, czy dokument pomaga ustalić plan działania, czy też istnieje po prostu dlatego, że jest wymogiem prawnym.

Sprawdzenie, czy zmiany skuteczności działania organizacji w zakresie bezpieczeństwa spowodowały przegląd strategii w zakresie bezpieczeństwa.

Sprawdzenie czy strategia w zakresie bezpieczeństwa odzwierciedla rzeczywistość organizacji.

## 2.3 Funkcje, odpowiedzialność, rozliczalność i uprawnienia w ramach organizacji

### 2.3.1 Wymóg regulacyjny

|  |
|--|
| <p>2.3.1. Odpowiedzialność, rozliczalność i uprawnienia pracowników pełniących funkcje, które mają wpływ na bezpieczeństwo (w tym kadry kierowniczej oraz pozostałego personelu zaangażowanego w zadania związane z bezpieczeństwem), są definiowane dla każdego szczebla hierarchii służbowej w obrębie organizacji, zostają udokumentowane oraz są przypisane i komunikowane tym pracownikom.</p> <p>2.3.2. Organizacja zapewnia, by pracownicy, którym powierzono odpowiedzialność za zadania związane z bezpieczeństwem, posiadali uprawnienia, kompetencje i odpowiednie zasoby na potrzeby wykonywania swoich zadań, bez bycia narażonym na negatywny wpływ działań innych funkcji biznesowych.</p> <p>2.3.3. Powierzenie odpowiedzialności za zadania związane z bezpieczeństwem musi zostać udokumentowane, podane do wiadomości odpowiednich pracowników, zaakceptowane i zrozumiane.</p> <p>2.3.4. Organizacja musi opisać przypisanie funkcji, o których mowa w pkt 2.3.1, do poszczególnych funkcji biznesowych w obrębie organizacji oraz – w stosownych przypadkach – poza organizacją (zob. pkt 5.3 Wykonawcy, partnerzy i dostawcy).</p> |
|--|

### 2.3.2 Cel

Celem tego wymogu jest uzyskanie od wnioskodawcy jasnego obrazu struktury organizacji oraz sposobu przydzielania funkcji i odpowiedzialności oraz utrzymywania ich w długim okresie od osób zajmujących pierwszoplanowe stanowiska do kadry kierowniczej wyższego szczebla. Jest to klucz do zrozumienia, jak dobrze system zarządzania bezpieczeństwem organizacji kontroluje ryzyko. Wnioskodawca powinien wykazać, w jaki sposób przydziela kompetentnych pracowników do działań, w jaki sposób zapewnia jasne rozumienie funkcji i odpowiedzialności przez tych pracowników oraz w jaki sposób pracownicy są rozliczani ze swoich wyników.

### 2.3.3 Noty wyjaśniające

Może istnieć rozbieżne rozumienie przepisów dotyczących zarządzania bezpieczeństwem na poziomie operacyjnym i procesów zarządzania, które mają kierować systemem zarządzania bezpieczeństwem (np. ocena ryzyka, monitorowanie). Określenie funkcji istotnych w systemie zarządzania bezpieczeństwem (**2.3.1**) nie ogranicza się do osób rozliczalnych z zarządzania procesami bezpieczeństwa i za nie odpowiedzialnych, takich jak kierownik ds. bezpieczeństwa lub zespół ds. bezpieczeństwa, ale obejmuje każdą funkcję w zadaniach związanych z bezpieczeństwem, np. personel operacyjny, i nie zależy od stanowisk należących lub nienależących w organizacji do kadry kierowniczej (tj. kadra kierownicza wyższego szczebla, bezpośredni przełożeni, inni pracownicy).

„Powierzenie” (**2.3.3**) oznacza przeniesienie odpowiedzialności na niższe stanowisko z wyższego stanowiska, zwykle w celu przyspieszenia reakcji organizacji na pojawiające się kwestie. Odpowiedzialność za bezpieczeństwo może być powierzana, tj. przekazywana kaskadowo, w ramach określonych obowiązków zawodowych, pod warunkiem udokumentowania takiego powierzenia. Rozliczalność za bezpieczeństwo nie może być powierzana i zgodnie z prawem spoczywa na kadrze kierowniczej wyższego szczebla. Określa ona obowiązek wykazania zadowolającego wypełnienia obowiązków dotyczących bezpieczeństwa przez osobę, której powierzono odpowiedzialność, jeżeli coś nie zostało wykonane, nie działa lub nie osiąga swojego celu.

Przypisanie funkcji (**2.3.4**) można wykazać poprzez dostarczenie odpowiedniego schematu organizacyjnego.

### ***Jak uwzględnia się czynniki ludzkie i organizacyjne oraz kulturę bezpieczeństwa?***

W ramach funkcji, obowiązków, odpowiedzialności i uprawnień, które powinny zdefiniować **(2.3.1)** wymianę informacji związanych z bezpieczeństwem. Na przykład, kto jest odpowiedzialny za informowanie maszynistów o zmianach. **(Zob. również 4.4.1 i 4.4.2).**

System zarządzania bezpieczeństwem powinien być zgodny z wymogami CSM w zakresie systemu zarządzania bezpieczeństwem **[1.1 lit. d)]**, a kadra kierownicza wyższego szczebla odpowiada za zapewnienie ich spełnienia przez system zarządzania bezpieczeństwem. Kadra kierownicza wyższego szczebla może powierzyć część swoich obowiązków odpowiednim pracownikom. Sprawozdawczość dotyczącą wyników prowadzi się zgodnie z wymogami przeglądu dokonywanego przez kierownictwo **(6.3)**, w przypadku którego odpowiedni pracownicy odpowiadają za informowanie kadry kierowniczej wyższego szczebla o skuteczności działania systemu zarządzania bezpieczeństwem.

„Zadania związane z bezpieczeństwem” **(2.3.1)** nie ograniczają się do tych zadań, które bezpośrednio zarządzają bezpieczeństwem (tj. czynności o istotnym znaczeniu dla bezpieczeństwa wykonywanych przez pracowników, gdy kontrolują lub wpływają na ruch pociągu, co może mieć wpływ na zdrowie i bezpieczeństwo osób, zgodnie z TSI OPE). Obejmują również zadania niezwiązane z realizacją przewozów, które są związane z oceną ryzyka (np. planowanie operacji, ustalanie harmonogramu pracy personelu, przydzielanie pojazdów). W przypadku uwzględnienia nowych lub zmienionych ról i obowiązków przeprowadza się analizę kwestii związanych z czynnikiem ludzkim w odniesieniu do zmiany i sposobu faktycznego wykonywania obowiązków w organizacji.

Istnieją kryteria powierzania i przydzielania zadań i obowiązków w przypadku stwierdzenia, że niezbędne są określone kompetencje i umiejętności. Kryteria te są stosowane, w związku z czym zadania w zakresie bezpieczeństwa są wyraźnie przypisane, a wykonujący je pracownicy posiadają odpowiednie kompetencje, uprawnienia i zasoby niezbędne do ich wykonywania oraz są świadomi zagrożeń związanych z ich zadaniami.

Podanie do wiadomości i zaakceptowanie zadań **(2.3.3)**, w tym zadań związanych z bezpieczeństwem, jest częścią normalnego procesu biznesowego określającego sposób powierzania pracownikom funkcji i powinno podlegać audytowi. W przypadku powierzenia obowiązków odbywa się to w sposób systematyczny.

Kadra kierownicza powinna posiadać wystarczającą wiedzę i zrozumienie kwestii czynników ludzkich i organizacyjnych, aby w razie potrzeby zapewnić zaangażowanie specjalistów. Funkcje, odpowiedzialność i rozliczalność specjalistów w zakresie czynników ludzkich i organizacyjnych należy określać odpowiednio do zadań do wykonania. **(2.3.3).**

Powinien istnieć proces zapewniający osobom fizycznym możliwość zgłaszania wypadków, których uniknięto, incydentów i wypadków bez obawy o konsekwencje. Strategia wspiera prawa i obowiązki jednostki w zakresie podnoszenia kwestii bezpieczeństwa i nie toleruje nękania, zastraszania, odwetu ani dyskryminacji z tego tytułu. Kluczem do sukcesu zasady „just culture” jest zaufanie i otwartość w organizacji. Buduje się je przez długi czas i zależą one od chęci kadry kierowniczej do przeprowadzenia kompleksowych analiz w przypadku wystąpienia incydentów i wypadków, a także do słuchania i wyciągania wniosków przed podejmowaniem reakcji. Konsekwencja w rozwiązywaniu problemów związanych z bezpieczeństwem jest ważna dla ustanowienia zasady „just culture”.

#### ***2.3.4 Dowody***

- *Schemat organizacyjny i odpowiedni tekst objaśniający przedstawiający strukturę organizacji odpowiedzialnej za bezpieczeństwo oraz sposób, w jaki przygotowano system zarządzania bezpieczeństwem, i to, jak łączy się on z kontekstem organizacji; **(2.3.1), (2.3.4)***
- *lista innych informacji określających szczegółowo obowiązki dotyczące bezpieczeństwa w strukturze organizacji; **(2.3.1), (2.3.3)***



- dowody na istnienie i prowadzenie systemu zarządzania kompetencjami dla wszystkich pracowników, który ocenia adekwatność zadań do przypisanych obowiązków, kompetencji i zasobów; **(2.3.2)**
- dowody z systemu zarządzania kompetencjami lub innych procedur kadrowych, takich jak zarządzanie wynikami, które zapewnia organizacja, że role i obowiązki są podawane do wiadomości pracowników, akceptowane i dobrze przez nich rozumiane oraz że pracownicy będą ponosić odpowiedzialność za ich wykonanie; **(2.3.3)**
- opis obowiązków w zakresie eksploatacji i utrzymywania, w tym definicja wymagań, które powinni spełniać odpowiednio pracownicy i wykonawcy; **(2.3.4)**
- w strategii dotyczącej czynników ludzkich i organizacyjnych należy wykazać wymogi dotyczące tego, kiedy i jak korzysta się z wiedzy fachowej na temat czynników ludzkich i organizacyjnych oraz jakie są ich funkcje i obowiązki. **(2.3.1), (zob. również 4.6)**

### 2.3.5 Przykłady dowodów

Schemat organizacyjny poparty dodatkowym tekstem, który pozwala podmiotowi oceniającemu zobaczyć, jaką strukturę ma system zarządzania bezpieczeństwem i w jaki sposób poszczególne części odnoszą się do siebie.

Odniesienie do systemu zarządzania kompetencjami (CMS) wraz z informacją o jego strukturze i łączami do miejsca, w którym można znaleźć informacje szczegółowe, w tym opisy pomocniczych procesów kadrowych, takich jak zarządzanie wynikami.

Zapewniono proces przedstawiania uwag, który stosuje się w celu zapewnienia dobrego zrozumienia informacji przekazywanych w ramach organizacji.

Uwzględnienie czynników ludzkich i organizacyjnych oraz poprawa kultury bezpieczeństwa będą miały pozytywny wpływ na spełnienie odpowiedniego wymogu systemu zarządzania bezpieczeństwem, a dowody na to można znaleźć w następujących źródłach:

Struktura organizacyjna jest spójna, a obowiązki są wyraźnie rozdzielone między pracownikami w całej organizacji.

Ogólne strategie i procedury dotyczące ról i obowiązków są spójne w całej organizacji.

Proces opisujący sposób przydzielania obowiązków dotyczących bezpieczeństwa, a przy dopuszczalnych przypadkach powierzenia odpowiedzialności oraz kilka przykładów pokazujących, jak ten proces funkcjonuje z wyraźnym odniesieniem do ustaleń dotyczących oceny ryzyka.

Przykłady opisów stanowisk odpowiedzialnych za wykonywanie zadań związanych z bezpieczeństwem oraz tych, które nie są bezpośrednio związane z eksploatacją i mają pośredni wpływ na wykonywanie działalności (tj. przypisywanie zadań, planowanie działalności i dostarczanie informacji operacyjnych pracownikom, nadzorowanie działalności) są dostępne i poddawane przeglądowi, o ile to konieczne (np. w przypadku zmiany harmonogramów).

System zarządzania bezpieczeństwem zawierający dowody na to, że obowiązki i ryzyko związane z zadaniami są uwzględnione w systemie zarządzania kompetencjami oraz w programach szkoleniowych. Istnieją dowody (np. osoba, której powierzono odpowiedzialność, potwierdziła to na piśmie), że obowiązki zostały formalnie przyjęte.

Procedura(-y) określająca(-e), jakie kompetencje i zasoby są wymagane, aby wspierać zadania i obowiązki w zakresie bezpieczeństwa na wszystkich poziomach hierarchii.

Strategia dotycząca czynników ludzkich i organizacyjnych pokazująca, w jaki sposób czynniki te są zintegrowane z procesami i projektami. Doświadczenie i działania związane z czynnikami ludzkimi i organizacyjnymi są odpowiednie do wielkości procesu lub projektu. W procesie lub planie projektu

określono funkcje i odpowiedzialność oraz rozliczalność, a także etapy, na których należy skorzystać z usług specjalisty ds. czynników ludzkich.

#### 2.3.6 *Odniesienia i normy*

- [Rozliczalność i odpowiedzialność za bezpieczeństwo](#) (SKYbrary)

#### 2.3.7 *Kwestie związane z nadzorem*

W przypadku nadzoru kluczowymi sprawami będą tutaj kwestie stopnia. Pytanie, na które należy odpowiedzieć, brzmi „w jakim stopniu dostarczone informacje odzwierciedlają rzeczywistą sytuację w praktyce”?

Analiza funkcjonowania systemu zarządzania kompetencjami pozwoli odpowiedzieć na większość pytań w tej sekcji.

## 2.4 Konsultacje z pracownikami i innymi stronami

### 2.4.1 Wymóg regulacyjny

- 2.4.1. W stosownych przypadkach należy konsultować się z pracownikami, ich przedstawicielami oraz zewnętrznymi zainteresowanymi stronami przy opracowywaniu, utrzymywaniu i doskonaleniu systemu zarządzania bezpieczeństwem w odniesieniu do poszczególnych części, za które są oni odpowiedzialni, w tym w odniesieniu do aspektów bezpieczeństwa procedur operacyjnych.
- 2.4.2. Organizacja ułatwia konsultacje z pracownikami poprzez zapewnienie metod i środków angażowania pracowników, rejestrowania ich opinii oraz przedstawiania uwag na temat tych opinii.

### 2.4.2 Cel

Wnioskodawca powinien udowodnić, że aktywnie angażuje swoich pracowników (lub ich przedstawicieli), a także zewnętrzne zainteresowane strony w wykorzystywanie i rozwijanie systemu zarządzania bezpieczeństwem w celu kontrolowania ryzyka w długim okresie. Będzie to również wskazówka dla organu oceniającego, jaka jest kultura bezpieczeństwa w organizacji oraz w jaki sposób aktywnie angażuje ona odpowiednie osoby trzecie w zarządzanie bezpieczeństwem w obszarach, w których ryzyko jest dzielone.

Organizacja przyznaje, że żadna osoba nie posiada wszystkich informacji potrzebnych do zarządzania bezpieczeństwem w sposób zrównoważony. Eksperti ds. procesów, eksperti ds. bezpieczeństwa, służby pomocnicze, pracownicy pierwszego kontaktu, kadra kierownicza i nadzorcy, związki zawodowe, zewnętrznymi wykonawcy, wszyscy posiadają i wykorzystują wiedzę i informacje niezbędne dla bezpieczeństwa. Muszą oni mieć możliwość spotkania się, przedyskutowania i wyrażenia swoich poglądów, aby jak najlepiej zrozumieć rzeczywistość miejsca pracy. Szczególną uwagę należy zwrócić na organizacyjne obszary współdziałania między służbami, działami i organizacjami. Należy wspierać wymianę pomysłów i informacji dotyczących analizy i postępowania z ryzykiem, wypadkami i incydentami.

Zaangażowanie w zgłaszanie informacji o istotnym znaczeniu dla bezpieczeństwa oraz udział w analizie niebezpiecznych sytuacji i incydentów odbywają się w atmosferze zaufania. Ponadto aktywnie dąży się do wczesnego poznania uwag personelu operacyjnego podczas oceny ryzyka, projektowania lub przekształcania instalacji technicznych i pisanie nowych procedur.

### 2.4.3 Noty wyjaśniające

Strony zewnętrzne (**2.4.1**) oznaczają organizacje, które mają styczność z wnioskodawcą, takie jak wykonawcy, partnerzy, dostawcy, odpowiednie agencje rządowe, władze lokalne lub służby ratownicze.

#### **Jak uwzględnić czynniki ludzkie i organizacyjne oraz kulturę bezpieczeństwa?**

Konsultacje z tymi zewnętrznymi stronami (**2.4.1**) mogą dotyczyć kwestii związanych z systemem zarządzania. Na przykład wykonawcy mogą odpowiadać za niektóre zadania związane z bezpieczeństwem, takie jak przygotowanie pociągu czy utrzymanie infrastruktury. W przypadku oceny ryzyka związanego z procedurą przygotowania pociągu lub utrzymaniem infrastruktury dobrą praktyką jest zaangażowanie tych wykonawców w dany proces.

Wiedza fachowa użytkowników końcowych jest ważna dla zapewnienia dobrego zrozumienia warunków pracy i procedur, procesów, narzędzi i dokumentacji zgodnych z ich przeznaczeniem. Konsultacje z pracownikami pierwszej linii, począwszy od oceny ryzyka po wybór i testowanie dokumentacji lub sprzętu,

pomogą opracować zrównoważone i bezpieczne działanie (przy lepszym przestrzeganiu zasad przez pracowników).

Rozwój pozytywnej kultury bezpieczeństwa jest wspierany dobrej jakości i terminowym przekazywaniem istotnych informacji tym, którzy powinni je otrzymać.

#### 2.4.4 Dowody

- Wnioskodawca powinien przedstawić szczegółowe informacje dotyczące procesu konsultacji z pracownikami (lub ich przedstawicielami) i odpowiednimi zewnętrznymi zainteresowanymi stronami, w tym w jaki sposób konsultacje te przekładają się na zmiany w systemie zarządzania bezpieczeństwem lub określonych procedurach operacyjnych; **(2.4.1), (2.4.2)**
- wnioskodawca powinien przedstawić informacje dotyczące stosowanego systemu w celu przekazywania pracownikom wyników konsultacji. **(2.4.2)**

#### 2.4.5 Przykłady dowodów

Proces lub procedura konsultacji z pracownikami (oraz, w stosownych przypadkach, ich przedstawicielami) i zainteresowanymi stronami przy opracowywaniu systemu zarządzania bezpieczeństwem.

Uwzględnienie czynników ludzkich i organizacyjnych oraz poprawa kultury bezpieczeństwa będą miały pozytywny wpływ na spełnienie odpowiedniego wymogu systemu zarządzania bezpieczeństwem, a dowody na to można znaleźć w następujących źródłach:

Przykłady protokołów ze spotkań konsultacyjnych z pracownikami (lub ich przedstawicielami) wraz z zapisem wyników.

Przykłady sposobu zbierania opinii i sugestii pracowników podczas procesu zarządzania zmianą (tj. w sprawie projektu/zmiany/nowej procedury operacyjnej) i sposobu ich uwzględniania.

Dokument/procedura pokazująca, w jaki sposób personel operacyjny, który będzie pracował w nowym lub zmienionym systemem technicznym, jest zaangażowany na wczesnym etapie (planowanie i rozwój) pracy, w celu zebrania danych, np. dotyczących interfejsu człowiek-maszyna.

Procedury określające, w jaki sposób w organizacji należy uwzględniać czynniki ludzkie i organizacyjne i komunikować wyniki związane z celami biznesowymi organizacji i procesami, np. projekty, dochodzenia dotyczące incydentów i wypadków, analizy ryzyka i inne działania związane z bezpieczeństwem dla pracowników, wykonawców, partnerów i dostawców.

Organizacja jasno określająca oczekiwania w zakresie bezpieczeństwa i wymagane zachowania. Priorytety organizacyjne są dostosowane, aby uniknąć sprzecznych celów. Opisano proces planowania, oceny ryzyka i kontrolowania działań mających na celu zapewnienie, że bezpieczeństwo nie jest zagrożone przez inne interesy, na przykład stosując konserwatywne podejmowanie decyzji. Cele związane z bezpieczeństwem są związane z kulturą bezpieczeństwa. Kadra kierownicza odgrywa czynną rolę w planowaniu i wdrażaniu potrzebnych zmian w kulturze bezpieczeństwa.

#### 2.4.6 Kwestie związane z nadzorem

Konsultacje z odpowiednimi pracownikami i ich zaangażowanie, zarówno wewnątrz, jak i na zewnątrz, są ważną częścią upewniania się, że osoby posiadające odpowiednie doświadczenie mogą mieć pozytywny wpływ na system zarządzania bezpieczeństwem w organizacji.

Nadzór w tym obszarze należy ukierunkować na zapisy dotyczące sposobu konsultacji z pracownikami i zewnętrznymi stronami oraz uwzględniania ich uwag, a także na zapisy dotyczące zmian w systemie zarządzania bezpieczeństwem, które powstały w tej dziedzinie.

Szczególną uwagę należy zwrócić na sposób, w jaki przekazuje się informacje zwrotne, a także na wyciąganie z nich wniosków.

Usprawnianie funkcjonowania  
systemu kolejowego  
na rzecz społeczeństwa.

### 3 Planowanie

#### 3.1 Działania mające na celu ograniczenie ryzyka

##### 3.1.1 Wymóg regulacyjny

###### 3.1.1. Ocena ryzyka

###### 3.1.1.1. Organizacja musi:

- (a) wskazać i poddać analizie wszystkie ryzyka operacyjne (w tym związane z działaniami człowieka), organizacyjne i techniczne istotne dla rodzaju (**charakteru**), zakresu i obszaru działalności prowadzonej przez organizację. Ryzyka takie obejmują ryzyka wynikające z czynników ludzkich i organizacyjnych, takich jak obciążenie pracą, organizacja pracy, zmęczenie lub odpowiedniość procedur oraz działalność innych zainteresowanych stron (zob. pkt 1. Kontekst organizacji);
- (b) oszacować ryzyka, o których mowa w lit. a), w drodze zastosowania odpowiednich metod oceny ryzyka;
- (c) opracować i wdrożyć środki bezpieczeństwa, wraz z określeniem powiązanych obowiązków (zob. pkt 2.3 Funkcje, odpowiedzialność, rozliczalność i uprawnienia w ramach organizacji);
- (d) opracować system monitorowania skuteczności środków bezpieczeństwa (zob. pkt 6.1 Monitorowanie);
- (e) zidentyfikować potrzebę współpracy, w stosownych przypadkach, z innymi zainteresowanymi stronami (takimi jak przedsiębiorstwa kolejowe, zarządcy infrastruktury, producenci, dostawcy usług utrzymania, podmioty odpowiedzialne za utrzymanie, dysponenci pojazdów kolejowych, usługodawcy i podmioty zamawiające) w odniesieniu do wspólnych ryzyk oraz wdrożenia odpowiednich środków bezpieczeństwa;
- (f) poinformować pracowników i zaangażowane podmioty zewnętrzne o ryzykach (zob. pkt 4.4 Informowanie i komunikowanie).

3.1.1.2 Dokonując oceny ryzyka, organizacja uwzględnia potrzebę określenia, zapewnienia i utrzymania bezpiecznego środowiska pracy odpowiadającego wymogom obowiązujących przepisów, w szczególności dyrektywy Rady 89/391/EWG.

###### 3.1.2. Planowanie zmiany

3.1.2.1. Organizacja musi określić potencjalne ryzyka dla bezpieczeństwa oraz odpowiednie środki bezpieczeństwa (zob. pkt 3.1.1 Ocena ryzyka) przed wdrożeniem zmiany (zob. pkt 5.4 Zarządzanie zmianą) zgodnie z procesem zarządzania ryzykiem określonym w rozporządzeniu (UE) nr 402/2013, obejmującym uwzględnienie ryzyk dla bezpieczeństwa wynikających z samego procesu zmiany.

### 3.1.2 Cel

Wymóg ten dotyczy sedna systemu zarządzania bezpieczeństwem, ma na celu skłonienie wnioskodawcy do wykazania, w jaki sposób jego systemy identyfikują i kontrolują ryzyko, które napotykają. Wymaga również od wnioskodawcy wykazania, w jaki sposób w praktyce wykorzystuje wyniki oceny ryzyka w celu poprawy kontroli ryzyka i sposobu, w jaki sprawdza to w długim okresie. Należy pamiętać, że wymóg ten nie dotyczy bezpośrednio zarządzania ryzykiem wynikającym ze zmian (co jest kolejnym wymogiem), ale jest z nim związany. Należy również zauważyć, że istnieje szczególny wymóg, który należy uwzględnić poprzez kwestie oceny ryzyka związane z działaniami człowieka, takie jak organizacja pracy i zarządzanie ryzykiem zmęczenia.

Wnioskodawca ma opisać we wniosku sposób organizacji i przekazywania tych informacji w ramach systemu zarządzania bezpieczeństwem, a treść powinna odzwierciedlać ryzyko, na jakie narażona jest organizacja, biorąc pod uwagę rodzaj, zasięg i obszar jej działalności (zob. kontekst organizacji). Należy zająć się zarówno ryzykiem, za które odpowiedzialność spoczywa na wnioskodawcy, jak i ryzykiem wynikającym z działań osób trzecich.

Powszechne zrozumienie w całej organizacji sposobu zapobiegania poważnym zagrożeniom uważa się za kwestię priorytetową dla dobrego zarządzania bezpieczeństwem. Niska częstotliwość występowania scenariusza nie powinna prowadzić do jego ignorowania. Co więcej, aby zapewnić realizm wybranego scenariusza oceny ryzyka w porównaniu z rzeczywistymi operacjami, zarówno eksperci ds. zarządzania bezpieczeństwem, jak i operatorzy mający do czynienia z najtrudniejszymi aspektami działalności uczestniczą w analizie bezpieczeństwa i ocenie ryzyka. Wyniki tych ocen przekazuje się w przystępnej i zrozumiałej formie wszystkim podmiotom przyczyniającym się do poprawy bezpieczeństwa. Kadra kierownicza sprzyja dyskusjom dotyczącym poważnych zagrożeń, które wymagają zarządzania, aby zapewnić wspólne zrozumienie i świadomość. Ponadto przez cały cykl życia systemu kładzie się nacisk na istnienie poważnych zagrożeń.

### 3.1.3 Noty wyjaśniające

Do celów oceny wniosku wnioskodawca powinien wykazać, w jaki sposób zapewnia zgodność z dyrektywą Rady 89/391/EWG i związanymi z nią przepisami. Ocena skupi się na wykazaniu zarządzania tymi kwestiami, a nie na samych kwestiach. Problemy, takie jak zarządzanie zmęczeniem lub stresem, a także sprawdzanie sprawności fizycznej i psychicznej można traktować jako problem prawny w ramach bezpieczeństwa i higieny pracy, jednak mają one wspólną płaszczyznę z systemem zarządzania kompetencjami (np. w przypadku szkoleń po dłuższej nieobecności) oraz z przydzielaniem zadań (pracowników należy przypisywać do określonych zadań dopiero po upewnieniu się, że są do nich odpowiedni), jak określono w TSI OPE.

W punkcie 3.1.1.1 lit. a) tekstu prawnego znajdującego się powyżej dla zarządcy infrastruktury słowo „rodzaj” zastępuje się słowem „charakter” do celów oceny.

„Działalność” [3.1.1.1 lit. a)] oznacza tu zarówno czynność, którą zainteresowane strony (wykonawcy, dostawcy i inni) wykonują w imieniu wnioskodawcy lub w porozumieniu z nim, jak również aktywa wykorzystywane na wspieranie tych czynności. Kluczową kwestią jest to, że wnioskodawca musi wykazać, że dysponuje solidnym procesem oceny ryzyka i że uwzględni wszystkie istotne zagrożenia. Niektóre zagrożenia (np. zagrożenia hydrogeologiczne, zagrożenia na przejazdach kolejowych, kamienie rzucone w pociągi, wtargnięcia) wymagają również uwzględnienia przez organizację, gdy jest to właściwe i uzasadnione. Kwestie te są jednak związane z ryzykiem operacyjnym (ponieważ wszystkie mają wpływ na ruch pociągów) i mogą nie być związane wyłącznie z działaniami człowieka.

„Inne zainteresowane strony” oznaczają zarówno organizacje, jak i osoby. Strony te mogą być poza systemem kolejowym [1.1. lit. c)].

Zmiana może być związana z bezpieczeństwem lub też nie (**3.1.2.1**). Należy ocenić wpływ wszelkich zmian związanych z bezpieczeństwem i określić odpowiednie środki bezpieczeństwa w celu ograniczenia związanych z nimi zagrożeń do dopuszczalnego poziomu. Wdrożenie procesu zarządzania zmianą może również prowadzić do zagrożeń dla bezpieczeństwa, w szczególności w przypadku decyzji o odroczeniu wdrożenia zmiany, gdy konieczne będzie uniknięcie, częściowo lub w całości, stworzenia kolejnego zagrożenia dla bezpieczeństwa. Zarządzanie ryzykiem (**3.1.1.1**) nie jest jednak wyłącznym elementem zarządzania zmianą. Zasadniczo organizacja powinna zapewnić odpowiednie zarządzanie zagrożeniami dla bezpieczeństwa związanymi z jej działalnością. Potrzeba zidentyfikowania tych zagrożeń dla bezpieczeństwa, zarządzania nimi i kontrolowania ich, w ramach systemu zarządzania bezpieczeństwem wnioskodawcy, wykracza zatem poza zarządzanie zmianą i stosowanie CSM w zakresie wyceny i oceny ryzyka.

CSM w zakresie wyceny i oceny ryzyka ma zastosowanie do wszystkich zmian technicznych, eksploatacyjnych lub organizacyjnych (które mają wpływ na eksploatację lub utrzymanie). W odniesieniu do każdej zmiany związanej z bezpieczeństwem wnioskodawca musi najpierw zdecydować, czy zmiana jest znacząca (czy też nie). Jeżeli zostanie uznana za znaczącą, musi wykazać, że ryzyko związane ze zmianą jest dopuszczalne, stosując zasady opisane w CSM, oraz że wynikające z tej oceny wymogi zostały skutecznie wdrożone w systemie podlegającym zmianom. Przeprowadzona ocena ryzyka jest następnie poddawana niezależnej ocenie lub ocenie uznanego organu, który sporządzi sprawozdanie dotyczące dopuszczalności analizy lub jej braku. Krajowe organy ds. bezpieczeństwa uwzględniają takie sprawozdania w swoich działaniach nadzorczych, ale nie mogą kwestionować wyników sprawozdania, chyba że mają powód, by sądzić, że procesu oceny ryzyka nie przeprowadzono prawidłowo. W przypadku gdy zmiana jest związana z bezpieczeństwem, ale nie jest znacząca, wnioskodawca musi udokumentować swoją decyzję i nadal będzie musiał dokonać oceny ryzyka w ramach procesu zarządzania ryzykiem w zakresie systemu zarządzania bezpieczeństwem. W takim przypadku odpowiedzialność za wybór odpowiednich metod oceny ryzyka mających uzasadnić, że zastosowane przez niego środki kontroli ryzyka są odpowiednie, aby kontrolować powiązane ryzyko do dopuszczalnego poziomu, spoczywa na wnioskodawcy. Należy zauważyć, że chociaż przesłanką zastosowania CSM w zakresie wyceny i oceny ryzyka jest to, czy zmiana jest znacząca, czy też nie, organizacja może zdecydować o stosowaniu CSM w każdym przypadku, na przykład jeśli uzna, że ze względów biznesowych lub społecznych zmiana wymagała niezależnej oceny pracy wykonanej przez organizację. Dalsze informacje na temat zarządzania znaczącymi zmianami można znaleźć w przewodniku ERA dotyczącym wspólnej metody oceny bezpieczeństwa w zakresie oceny ryzyka.

CSM w zakresie wyceny i oceny ryzyka zawiera sześć kryteriów, które należy zbadać w celu określenia „znaczenia”. Są to:

- **skutki awarii:** wiarygodny najgorszy scenariusz w przypadku awarii ocenianego systemu, uwzględniający istnienie barier zabezpieczających poza systemem;
- **innowacja wykorzystana przy wprowadzaniu zmiany:** kryterium to obejmuje innowacje dotyczące zarówno całego sektora kolejowego, jak i organizacji wprowadzającej zmianę;
- **złożoność zmiany;**
- **monitoring:** niezdolność monitorowania wprowadzonej zmiany podczas całego cyklu życia systemu i dokonywania odpowiednich interwencji;
- **odwracalność zmiany:** niezdolność powrotu do systemu przed zmianą oraz
- **dotatkowość:** ocena znaczenia zmiany z uwzględnieniem wszystkich przeprowadzonych niedawno zmian ocenianego systemu, które były związane z bezpieczeństwem i nie zostały ocenione jako znaczące.

Elementy te należy wykorzystać do oceny sposobu podejmowania przez organizację decyzji dotyczących „znaczenia” w ramach CSM w zakresie wyceny i oceny ryzyka.

Chociaż proces zarządzania ryzykiem określony w CSM w zakresie wyceny i oceny ryzyka ma zastosowanie w przypadku istotnych zmian związanych z bezpieczeństwem, zasady będące podstawą procesu zarządzania



ryzykiem, ustanowione w tym rozporządzeniu, są powszechną praktyką w zakresie zarządzania ryzykiem i dlatego można je stosować we wszystkich innych sytuacjach, w których konieczna jest ocena ryzyka.

### **Jak uwzględnić się czynniki ludzkie i organizacyjne oraz kulturę bezpieczeństwa?**

Czynniki ludzkie i organizacyjne są stosowane konsekwentnie, od samego początku, podczas projektowania (nowych) systemów. Wszystkie szczeble organizacji, w tym operatorzy pierwszej linii, są zaangażowani w sposób proaktywny w ocenę ryzyka, przewidując wystąpienie błędów poprzez podejście skoncentrowane na użytkowniku, w którym struktura organizacyjna przedsiębiorstwa, dostępność/użytkowanie sprzętu, projektowanie zadań bezpieczeństwa, system zarządzania kompetencjami i procedury są brane pod uwagę przy ocenie ryzyka dla bezpieczeństwa i identyfikacji środków bezpieczeństwa.

Procedura oceny ryzyka będzie zawierała podejścia lub metody pozwalające na systematyczne uwzględnianie czynników ludzkich i organizacyjnych oraz dążenie do usunięcia ryzyka u źródła we wszystkich procesach i procedurach systemu zarządzania bezpieczeństwem, gdy jest to możliwe. Jeśli nie jest to możliwe, strategia dotycząca czynników ludzkich i organizacyjnych powinna zmierzać do minimalizacji skutków ryzyka.

Istnieje systematyczne podejście do określania zadań i procesów związanych z bezpieczeństwem, a metody z dziedziny czynników ludzkich i organizacyjnych stosuje się do analizy zadań o istotnym znaczeniu dla bezpieczeństwa, np. analiza zadań, HTA (hierarchiczna analiza zadań), TTA (tabelaryczna analiza zadań). Do wyboru i zastosowania właściwych metod należy wykorzystać wiedzę fachową na temat czynników ludzkich i organizacyjnych.

Proces oceny ryzyka powinien opisywać udział specjalistów ds. czynników ludzkich i organizacyjnych oraz odpowiednich kompetencji użytkowników i innych zainteresowanych stron. Może na przykład zawierać opis zakresu, w jakim specjaliści ds. czynników ludzkich i organizacyjnych powinni uczestniczyć w analizie ryzyka i konieczny poziom kompetencji w zakresie czynników ludzkich i organizacyjnych.

Opisano odpowiednie metody integracji czynników ludzkich i organizacyjnych w ocenie ryzyka, np. analiza zadań, analiza używalności, symulacja, HAZOP dotycząca ludzi, analiza muchy (bow-tie).

#### **3.1.4 Dowody**

- *Wnioskodawca powinien przedstawić dowody, że dysponuje procesem oceny ryzyka (w tym opis zastosowanej metodyki, uczestniczących pracowników oraz wszelkich dokonanych zatwierdzeń lub weryfikacji), który obejmuje zarówno ryzyko uznane za znaczące zmiany w ramach CSM w zakresie wyceny i oceny ryzyka (rozporządzenie wykonawcze Komisji (UE) nr 402/2013), jak i ryzyko uznane za nieznaczące, które mimo to wymaga kontroli, a proces obejmuje wszystkie ryzyka operacyjne, organizacyjne i techniczne; [3.1.1.1 lit. a), b)]*
- *dowody, że w ocenach ryzyka uwzględniono ryzyko związane z czynnikami ludzkimi i organizacyjnymi. Strategia dotycząca czynników ludzkich i organizacyjnych powinna pokazywać, jak i kiedy czynniki ludzkie i organizacyjne są integralną częścią procesu oceny ryzyka, i wskazywać zastosowanie odpowiednich metod i wiedzy fachowej; [3.1.1.1 lit. a)]*
- *dowody na to, że w procesie oceny ryzyka w stosownych przypadkach uczestniczą osoby trzecie, w tym sposób zarządzania ryzykiem ze strony osób trzecich, które mają wpływ na działalność przedsiębiorstwa kolejowego lub zarządcy infrastruktury; [3.1.1.1 lit. a)], [3.1.1.1 lit. e)], [3.1.1.1 lit. f)]*
- *dowody, że wnioskodawca wdrożył proces opracowywania i wprowadzania środków kontroli ryzyka, w tym kto odpowiada za zapewnienie ich zakończenia; [3.1.1.1 lit. c)].*
- *wnioskodawca powinien wskazać, w jaki sposób uwzględnić i przekazuje wyniki oceny ryzyka oraz związane z nimi środki kontroli odpowiednim pracownikom; [3.1.1.1 lit. f)]*
- *wnioskodawca powinien wykazać, w jaki sposób monitoruje skuteczność swoich środków kontroli ryzyka, w tym w jaki sposób aktualizuje zgodnie z wymogami procesy lub procedury; [3.1.1.1 lit. d)]*

- w przedstawionych dowodach wnioskodawca powinien wskazać, w jaki sposób uwzględnia konieczność przestrzegania innych mających zastosowanie przepisów, takich jak przepisy wydane na mocy dyrektywy Rady 89/391/EWG; **(3.1.1.2)**
- wnioskodawca przedstawia dowody mające wykazać w ramach procesu zarządzania zmianą, że wpływ każdej zmiany jest systematycznie oceniany. Będzie to oznaczać wykorzystanie oceny ryzyka, w tym wykorzystanie CSM w zakresie wyceny i oceny ryzyka, do określenia ryzyka i niezbędnych środków kontroli. Wnioskodawca przedstawia również dowody na to, że wdrożono środki kontroli określone podczas procesu zarządzania zmianą; **(3.1.2.1)**

### 3.1.5 Przykłady dowodów

Proces lub procedura oceny ryzyka uwzględniająca w stosownych przypadkach, w jaki sposób i kiedy stosuje się analizę przyczyn i skutków wad (FMEA), analizę zagrożeń i zdolności operacyjnych (HAZOP) lub inne techniki mające wspierać wdrażanie środków kontroli służących przeciwdziałaniu ryzyku.

Dowód w postaci rejestru zagrożeń, który pokazuje, że organizacja stosuje proces systematycznej oceny zagrożeń, stanowiący pierwszy etap oceny ryzyka. Rejestr zagrożeń zawierający wyniki monitorowania jest aktualizowany niezwłocznie po wykryciu nowych zagrożeń, uzupełniany odpowiednimi informacjami dotyczącymi środków bezpieczeństwa przyjętych w celu utrzymania ryzyka pod kontrolą (np. sprzęt techniczny, wykazy elementów o istotnym znaczeniu dla bezpieczeństwa, procedury operacyjne, szkolenie pracowników).

Procedura zgodności z innymi odpowiednimi przepisami UE, takimi jak dyrektywa Rady 89/391/EWG w zakresie, w jakim ryzyko związane z personelem (śmierć, tymczasowe lub trwałe obrażenia, wypadki, których uniknięto) może być objęte ramami prawnymi bezpieczeństwa i higieny pracy, ale środki kontroli powinny być włączone do przepisów operacyjnych lub je uzupełniać.

Uwzględnienie czynników ludzkich i organizacyjnych oraz poprawa kultury bezpieczeństwa będą miały pozytywny wpływ na spełnienie odpowiedniego wymogu systemu zarządzania bezpieczeństwem, a dowody na to można znaleźć w następujących źródłach:

Przegląd elementów procesu określających sposób uwzględniania czynników ludzkich i organizacyjnych w procesie oceny ryzyka oraz sposób i przypadki konieczności angażowania osób trzecich. Protokoły z posiedzeń wskazują, że uczestniczyli w nich użytkownicy końcowi oraz eksperci ds. czynników ludzkich i organizacyjnych, a ich opinie były brane pod uwagę.

Przykłady przeprowadzonych analiz uwzględniających liczbę i charakter zadań do wykonania, ich złożoność, powtarzalność, delegowanie obowiązków, obciążenie pracą (w tym harmonogram, zmiany, wykorzystanie maszyn i odpowiednich instrukcji itp.), jasność i wyczerpujący charakter zasad i instrukcji pracy, informacje zwrotne od pracowników oraz sposób podejmowania działań naprawczych.

Procedura przekazywania pracownikom wyników ocen ryzyka, w stosownych przypadkach z ilustrującymi przykładami.

Wskazanie procesu mającego zapewnić, by zadania związane z bezpieczeństwem przekazywane każdej kategorii pracowników opracowywano w taki sposób, aby:

- liczba zadań do wykonania nie była zbyt duża w czasie wykonywania zadania związanego z bezpieczeństwem;
- jeśli zadania związane z bezpieczeństwem są połączone, organizacja była w stanie wykazać, że poziom bezpieczeństwa jest utrzymany;
- nie było sprzeczności między realizacją zadań związanych z bezpieczeństwem a innymi celami przydzielonymi pracownikom [zgodnie z 2.1.1 lit. j)].

Strategia dotycząca czynników ludzkich i organizacyjnych, która łączy się z procesami oceny ryzyka. Pokazuje ona, że wykorzystuje się wyniki analiz ryzyka oraz wdraża i ocenia środki zwiększające bezpieczeństwo

W przypadku niektórych elementów związanych z czynnikami ludzkimi i organizacyjnymi rozpatrywanymi w ramach prawnych dotyczących bezpieczeństwa i higieny pracy, a także w przypadku ważnych kwestii, takich jak zmęczenie, stres związany z pracą i fizyczne środowisko pracy (np. czystość, temperatura, światło) – w takich przypadkach dokumentacja dotycząca bezpieczeństwa i higieny pracy powinna być zarządzana w ramach systemu zarządzania bezpieczeństwem.

### 3.1.6 Odniesienia i normy

- [Przewodnik Agencji dotyczący stosowania CSM w zakresie oceny ryzyka](#)
- [Kryteria akceptacji ryzyka w odniesieniu do systemów technicznych i procedur operacyjnych stosowanych w różnych gałęziach przemysłu](#)
- [Wytyczne wspierające wdrażanie rozporządzenia \(UE\) 2015/1136 w sprawie zharmonizowanych wymagań projektowych w ramach CSM w zakresie oceny ryzyka](#)
- ISO 31000:2018 Zarządzanie ryzykiem
- ISO 31010:2019 Zarządzanie ryzykiem – Techniki oceny ryzyka
- ISO 45001:2018 Systemy zarządzania bezpieczeństwem i higieną pracy – praktyczny przewodnik dla małych organizacji
- CENELEC – EN50126 Zastosowania kolejowe – Specyfikowanie i wykazywanie niezawodności, dostępności, możliwości utrzymania i bezpieczeństwa (RAMS) Część 1: Wymagania podstawowe i procesy ogólnego przeznaczenia
- [Biuro krajowego organu regulacyjnego ds. bezpieczeństwa kolei \(Office of the National Rail Safety Regulator\) – Wytyczne dotyczące zarządzania aktywami \(2019\)](#)

### 3.1.7 Kwestie związane z nadzorem

Proces oceny ryzyka powinien być głównym elementem systemu zarządzania bezpieczeństwem podczas sprawowania nadzoru. Na podstawie przeprowadzonych wywiadów i kontroli dokumentacji i procesów powinno być zatem możliwe stwierdzenie, czy tak jest w rzeczywistości. Kluczowe znaczenie mają tutaj wszelkie ustalenia z nadzoru, które będą miały znaczenie dla przyszłego odnowienia jednolitego certyfikatu bezpieczeństwa lub autoryzacji bezpieczeństwa. Ponadto wszelkie ustalenia z nadzoru procesów oceny ryzyka powinny w razie potrzeby stanowić wkład w strategię nadzoru krajowego organu ds. bezpieczeństwa.

Poniższe informacje mogą stanowić dane wymagające późniejszego nadzoru:

- wykaz zagrożeń;
- wyniki analizy ryzyka, w tym w stosownych przypadkach sprawozdania organu lub organów oceny ryzyka;
- uzasadnienie dotyczące stosowania metod oceny ryzyka (np. FMECA, FTA, ETA, HAZOP), w tym sposobu ustalania kryteriów oceny ryzyka oraz określania dotkliwości zagrożenia i prawdopodobieństwa wystąpienia zagrożenia;
- odpowiednio, klasyfikacja zdarzeń niebezpiecznych według przedmiotu, skutków lub przyczyn (np. wykaz wstępnych zagrożeń).

Pracownicy odpowiedzialni za ocenę ryzyka powinni być świadomi swojej roli i znaczenia tego procesu oraz kompetentni do jego skutecznego wykonywania.

Szczególnie ważne jest zbadanie szeregu przykładów ocen ryzyka, ponieważ wykażą one, czy ryzyko jest właściwie rozpatrywane przy użyciu odpowiedniej metodyki. Obserwacja w terenie powinna następnie wykazać, że wprowadzono określone środki kontroli.

## 3.2 Cele w zakresie bezpieczeństwa i planowanie

### 3.2.1 Wymóg regulacyjny

- 3.2.1. Organizacja musi określić cele w zakresie bezpieczeństwa dla odpowiednich funkcji na odpowiednich poziomach w celu utrzymania oraz, gdy jest to wykonalne w sposób rozsądny, poprawy swoich wyników w zakresie bezpieczeństwa.
- 3.2.2. Cele w zakresie bezpieczeństwa muszą:
- (a) być spójne z polityką w zakresie bezpieczeństwa i celami strategicznymi organizacji (w stosownych przypadkach);
  - (b) być powiązane z najważniejszymi ryzykami mającymi wpływ na wyniki organizacji w zakresie bezpieczeństwa;
  - (c) być mierzalne;
  - (d) uwzględniać obowiązujące wymogi prawne i inne wymogi;
  - (e) być poddawane przeglądowi pod kątem ich osiągnięcia i w stosownych przypadkach zmieniane;
  - (f) być komunikowane.
- 3.2.3. Organizacja musi posiadać plan(y) opisujący(-e), w jaki sposób zamierza osiągnąć swoje cele w zakresie bezpieczeństwa.
- 3.2.4. Organizacja musi opisać strategię i plan(y) wykorzystywane do monitorowania osiągnięcia celów w zakresie bezpieczeństwa (zob. pkt 6.1 Monitorowanie).

### 3.2.2 Cel

Zapewnienie, by organizacja spełniała wymogi prawne i zapewniała przekazywanie koncepcji ciągłej poprawy bezpieczeństwa pracownikom i wiarę w nią kadry kierowniczej.

Wnioskodawca musi wykazać, że ma znaczące cele oraz proces ich wdrażania i monitorowania w ciągu całego cyklu życia.

### 3.2.3 Noty wyjaśniające

Skuteczność działania w zakresie bezpieczeństwa oznacza tutaj wyniki organizacji w odniesieniu do jej celów w zakresie bezpieczeństwa oraz skuteczność systemu zarządzania bezpieczeństwem i wszystkich procesów i procedur, które to wspierają.

Termin „cele w zakresie bezpieczeństwa” stosuje się wymiennie z terminem „wymagania bezpieczeństwa”, chociaż ten drugi ma zwykle znaczenie liczbowe. Cele w zakresie bezpieczeństwa lub wymagania bezpieczeństwa różnią się od wspólnych wymagań bezpieczeństwa ustalonych na szczeblu państw członkowskich, jednak niektóre przedsiębiorstwa mogą wykorzystywać te ostatnie jako cele, które należy osiągnąć, aby utrzymać lub poprawić swoją skuteczność działania w zakresie bezpieczeństwa.

Przy zastosowaniu podejścia planuj-wykonaj-sprawdź-działaj cele powinny być poddawane regularnym przeglądom i powinny uwzględniać wyniki oceny ryzyka oraz wcześniejsze monitorowanie i badanie wypadków i incydentów przy ustalaniu priorytetów w celu utrzymania i, w miarę możliwości, poprawy skuteczności działania w zakresie bezpieczeństwa.

Ustalanie i monitorowanie wskaźników skuteczności działania w zakresie bezpieczeństwa, które wspierają proces decyzyjny organizacji w zakresie kontroli ryzyka i, gdy są one skuteczne, są uwzględniane przy ustalaniu i przeglądzie celów w zakresie bezpieczeństwa.

### ***Jak uwzględnić czynniki ludzkie i organizacyjne oraz kulturę bezpieczeństwa?***

Cele w zakresie bezpieczeństwa są powiązane z zagrożeniami, ponieważ te drugie będą miały wpływ na skuteczność działania organizacji w zakresie bezpieczeństwa (tj. zamierzone wyniki systemu zarządzania bezpieczeństwem, a tym samym powodzenie w osiąganiu celów). Cele w zakresie bezpieczeństwa mogą być ilościowe, przedstawione w formie zmniejszenia liczby zdarzeń wyrażonego jako wartość bezwzględna lub procentowo. Cele w zakresie bezpieczeństwa mogą być również jakościowe, wyrażone jako wartość rodzajowa, np. „bezpieczeństwo na przejazdach kolejowych zostanie poprawione” lub „obecny poziom bezpieczeństwa zostanie utrzymany”. W tym przypadku jednak poziom poprawy lub poziom, na którym bezpieczeństwo zostanie utrzymane, będzie musiał być zdefiniowany i monitorowany zgodnie z określonymi kryteriami w celu ustalenia, czy cele w zakresie bezpieczeństwa są osiągnięte.

Organizacja definiuje cele SMART i przekazuje je pracownikom, aby rozwijać ich świadomość powagi i znaczenia ich działań oraz wkładu w realizację celów w zakresie bezpieczeństwa oraz planowania zarządzania zagrożeniami bezpieczeństwa. Pracownicy są również świadomi, że osiągnięcie celów jest monitorowane i w razie potrzeby poddawane przeglądowi.

Cele są traktowane priorytetowo na podstawie oceny ryzyka, zgodnie ze sobą i z polityką bezpieczeństwa.

#### ***3.2.4 Dowody***

- *Istnieje zestaw celów w zakresie bezpieczeństwa SMART, które wpisują w szersze potrzeby biznesowe organizacji; **[3.2.1), [3.2.2 lit. a), b), c)]***
- *oświadczenie wskazujące wymogi prawne i sposób ich spełniania; **[3.2.2 lit. d)]***
- *opis sposobu, w jaki można osiągnąć te cele i przekazać je odpowiednim pracownikom; **[3.2.2 lit. f)], (3.2.3)***
- *istnieje proces monitorowania celów, zgodny z wymogami określonymi we wspólnej metodzie oceny bezpieczeństwa w odniesieniu do monitorowania (rozporządzenie (UE) nr 1078/2012), mający zapewnić ich ciągłą przydatność do realizacji zamierzeń i osiągnięcia celów przez organizację. **[3.2.2 lit. e)], (3.2.4)***

#### ***3.2.5 Przykłady dowodów***

Opis procesu ustanawiania celów w zakresie bezpieczeństwa, określania ich priorytetów, monitorowania oraz sposobu unikania i, w przypadku braku możliwości uniknięcia, rozwiązywania konfliktów z innymi celami. Opis procesu powinien zawierać poziom, na którym ustalane są cele, oraz sposób, w jaki w razie potrzeby przyczyniają się one do realizacji innych celów na innych poziomach. Powinien także uwzględniać wspólne płaszczyzny, harmonogram i wszelkie niezbędne uzupełniające dane jakościowe lub ilościowe.

Cele w zakresie bezpieczeństwa i plan ich realizacji wraz z procesem, który będzie realizowany, gdy okaże się, że cele w zakresie bezpieczeństwa nie zostaną osiągnięte.

Cele w zakresie bezpieczeństwa są zgodne z deklaracjami misji i wizji określonymi w strategii w zakresie bezpieczeństwa i na tej podstawie można zauważyć, że są one cenione przez pracowników i zwiększają ich zaangażowanie w ich osiągnięcie.

Proces lub procedura pozwalająca przekształcić wyniki działań w zakresie monitorowania w cele w zakresie bezpieczeństwa, planowanie działań w celu ich osiągnięcia oraz powiązane wskaźniki realizacji.

Uwzględnienie czynników ludzkich i organizacyjnych oraz poprawa kultury bezpieczeństwa będą miały pozytywny wpływ na spełnienie odpowiedniego wymogu systemu zarządzania bezpieczeństwem, a dowody na to można znaleźć w następujących źródłach:

Plan strategiczny organizacji stawiający bezpieczeństwo jako cel nadrzędny.

Przepisy obowiązujące w ramach systemu zarządzania bezpieczeństwem (proces zarządzania ryzykiem), które wyjaśniają, jak należy postępować w przypadku sprzeczności między poszczególnymi celami.

Proces konsultacji z pracownikami w sprawie celów w zakresie bezpieczeństwa oraz proces określania i komunikowania indywidualnych celów w zakresie bezpieczeństwa, a także sposób ich formalnej akceptacji przez pracowników. Konieczne jest wprowadzenie procesu wyjaśniającego, gdzie cele mogą być znalezione przez pracowników, jak mogą dowiedzieć się o swoim oczekiwanym poziomie wkładu w osiągnięcie tych celów i jak są one przeglądane/mierzone pod kątem ich realizacji, opracowywane i planowane.

Procedura komunikowania celów pracownikom pokazuje, jak rozwijana jest świadomość i sprawdzane jest zrozumienie.

W procedurze sprawozdawczości, w ramach której pracownicy wskazują realizację celów bezpieczeństwa.

### 3.2.6 *Kwestie związane z nadzorem*

Kluczową kwestią wymagającą nadzoru będzie to, na ile wyznaczone cele są osiągalne w praktyce i co dzieje się w rzeczywistości, jeśli zacznie być jasne, że ich osiągnięcie jest mało prawdopodobne.

Sposób ustalania i przeprowadzania przeglądu celów w zakresie bezpieczeństwa – cele koncentrują się na wrażliwych lub krytycznych działaniach/kontrolach i korzystają ze wskaźników rezultatów i działań.

Sposób, w jaki organizacja wykazuje stałą poprawę kontroli ryzyka dzięki swoim celom w zakresie bezpieczeństwa.

Sposób skutecznego monitorowania przez organizację swojej skuteczności działania w zakresie bezpieczeństwa, a zatem wykorzystywania wspólnej metody oceny bezpieczeństwa w odniesieniu do monitorowania do oceny skuteczności w odniesieniu do celów w zakresie bezpieczeństwa i związanych z nimi wskaźników skuteczności działania w zakresie bezpieczeństwa.

Sposób, w jaki cele (np. cel określony kilka lat wcześniej) są opracowywane od momentu stworzenia do ostatecznego osiągnięcia (lub niepowodzenia).

Usprawnianie funkcjonowania  
systemu kolejowego  
na rzecz społeczeństwa.

## 4 Wsparcie

### 4.1 Zasoby

#### 4.1.1 Wymóg regulacyjny

4.1.1. Organizacja zapewnia zasoby, w tym kompetentnych pracowników oraz skuteczne i użyteczne wyposażenie, potrzebne do ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem.

#### 4.1.2 Cel

Celem tego wymogu jest upewnienie się, że organizacja wdrożyła procesy zapewniające odpowiednie zasoby, takie jak sprzęt techniczny lub systemy lub kompetentni pracownicy, aby umożliwić swojemu systemowi zarządzania bezpieczeństwem kontrolowanie ryzyka zgodnie z jego celami.

#### 4.1.3 Noty wyjaśniające

Przeznaczenie odpowiednich zasobów jest warunkiem wstępnym osiągnięcia odpowiedniego poziomu bezpieczeństwa.

#### **Jak uwzględnić czynniki ludzkie i organizacyjne oraz kulturę bezpieczeństwa?**

Przedsiębiorstwo zapewnia pracownikom niezbędne środki do bezpiecznego wykonywania zadań. Dotyczy to personelu, sprzętu i dokumentacji. Wymóg ten jest również związany z oceną ryzyka i określonymi środkami bezpieczeństwa.

#### 4.1.4 Dowody

- *Informacje dotyczące systemu zarządzania kompetencjami (CMS) lub w przypadku braku CMS dowody tego, w jaki sposób organizacja zapewnia posiadanie wystarczającej liczby kompetentnych pracowników; (4.1.1)*
- *informacje dotyczące sposobu, w jaki organizacja upewnia się, że posiada wystarczającą ilość użytecznego wyposażenia, aby mogła wypełnić swoje zobowiązania z tytułu świadczenia usług i utrzymać sprawny system zarządzania bezpieczeństwem zapewniający kontrolę ryzyka; (4.1.1)*
- *informacje dotyczące organizacji funkcji związanych z utrzymaniem (zob. również załącznik II rozporządzenia 2019/779 w sprawie podmiotów odpowiedzialnych za utrzymanie) oraz sposobu, w jaki funkcje te przyczyniają się do zapewnienia zasobów wystarczających do tego, by organizacja mogła wypełniać spoczywające na niej zobowiązania z tytułu świadczenia usług. (4.1.1)*

#### 4.1.5 Przykłady dowodów

Procedura zarządzania kompetencjami lub szczegółowe informacje na temat procesu służącego zapewnieniu powierzenia kompetentnym pracownikom organizacji odpowiednich funkcji, w stosownych przypadkach w połączeniu z organizowaniem szczegółowych ocen i programów szkoleniowych (**zob. również 4.2**).

Oświadczenie wskazujące proces przydzielania zasobów w sposób, który umożliwia zaspokojenie potrzeb operacyjnych, a także zawierające stosowne odniesienia do dokumentów uzupełniających.

Uwzględnienie czynników ludzkich i organizacyjnych oraz poprawa kultury bezpieczeństwa będą miały pozytywny wpływ na spełnienie odpowiedniego wymogu systemu zarządzania bezpieczeństwem, a dowody na to można znaleźć w następujących źródłach:

Oświadczenie wskazujące, w jaki sposób ustala się wymogi związane z personelem, tak aby zapewnić sprawne funkcjonowanie systemu zarządzania bezpieczeństwem, i zawierające szczegółowe informacje na temat odpowiednich procedur lub procesów referencyjnych dostarczających dodatkowych informacji w tym zakresie.

Proces wyjaśniający, w jaki sposób przydzielane są zasoby w wyniku oceny ryzyka i środków bezpieczeństwa, co do których podjęto decyzję o wykonaniu zadania: w tym czasie, personel, kompetencje (w tym umiejętności inne niż techniczne), procedury, narzędzia i sprzęt.

Wyniki analiz zadań pokazujące, że odpowiedni czas i personel określa się przy uwzględnieniu obciążenia pracą. Proces ten jest przeprowadzany w podobny sposób dla wszystkich zadań związanych z bezpieczeństwem we wszystkich jednostkach organizacyjnych („długodystansowe”/„krótkodystansowe” usługi transportowe, maszyniści, praca manewrowa, działalność w zakresie utrzymania...).

Dokument, w którym opisano zasoby przydzielone na potrzeby planowanych zmian w organizacji (w tym na politykę kadrową i dostawy niezbędnego wyposażenia).

#### 4.1.6 Kwestie związane z nadzorem

Należy sprawdzić, czy ramy kompetencji oraz wymogi dotyczące wyposażenia są w jasny sposób powiązane z wynikami oceny ryzyka.

Analizując system zarządzania kompetencjami, krajowy organ ds. bezpieczeństwa powinien sprawdzić, czy organizacja wdrożyła środki konieczne do wskazania i utrzymania personelu posiadającego właściwe umiejętności, które umożliwią mu wykonywanie przydzielonych zadań w bezpieczny sposób. W tym kontekście kluczowe znaczenie będzie miał proces aktualizowania systemu zarządzania kompetencjami.

Monitorując działania związane z utrzymaniem, powiązane z tym wymogiem, nadzorujący powinien sprawdzić, czy w przypadku powierzenia tych czynności podmiotom zewnętrznym przedsiębiorstwo kolejowe lub zarządca infrastruktury sprawuje nad nimi nadzór w celu zagwarantowania dostarczenia przez wykonawców odpowiedniego, bezpiecznego do stosowania produktu.

Monitorowanie wakatów na wybranych stanowiskach związanych z systemem zarządzania bezpieczeństwem może posłużyć za wskaźnik pomocny przy ocenianiu odpowiedniości zasobów ludzkich.

Podobnie sposób korzystania ze sprzętu – np. liczba sztuk zapasowych zabieranych na miejsce wykonywania czynności – może stanowić wyznacznik jakości zapewnianego sprzętu, a tym samym odpowiedniości zasobów.



## 4.2 Kompetencja

### 4.2.1 Wymóg regulacyjny

- 4.2.1. System zarządzania kompetencjami utrzymywany przez organizację musi zapewniać, by pracownicy pełniący funkcje mające wpływ na bezpieczeństwo byli kompetentni w odniesieniu do zadań związanych z bezpieczeństwem, za które są odpowiedzialni (zob. pkt 2.3 Funkcje, odpowiedzialność, rozliczalność i uprawnienia w ramach organizacji), i obejmować co najmniej:
- (a) określenie kompetencji (w tym wiedzy, umiejętności oraz zachowań i postaw o charakterze innym niż techniczny) wymaganych do celów zadań związanych z bezpieczeństwem;
  - (b) zasady selekcji (podstawowy poziom wykształcenia, wymagana sprawność psychiczna i fizyczna);
  - (c) początkowy poziom wykształcenia, doświadczenia i kwalifikacji;
  - (d) bieżące szkolenia i okresową aktualizację posiadanych kompetencji;
  - (e) okresową ocenę kompetencji oraz badania sprawności psychicznej i fizycznej, aby zapewnić utrzymanie kwalifikacji i umiejętności z upływem czasu;
  - (f) specjalistyczne szkolenia dotyczące odpowiednich części systemu zarządzania bezpieczeństwem, tak aby zapewnić wywiązywanie się z zadań związanych z bezpieczeństwem.
- 4.2.2. Organizacja musi zapewnić program szkoleń, o których mowa w pkt 4.2.1 lit. c), d) i f), dla pracowników wykonujących zadania związane z bezpieczeństwem, gwarantujący że:
- (a) program szkoleń jest realizowany zgodnie ze zidentyfikowanymi wymaganiami dotyczącymi kompetencji oraz indywidualnymi potrzebami pracowników;
  - (b) w stosownych przypadkach szkolenia zapewniają pracownikom umiejętność działania w każdych warunkach prowadzenia działalności (w warunkach normalnych, w sytuacji awarii oraz w sytuacji kryzysowej);
  - (c) czas trwania szkoleń oraz częstotliwość szkoleń odświeżających są odpowiednie do celów szkoleniowych;
  - (d) dla wszystkich pracowników prowadzona jest dokumentacja szkoleń (zob. pkt 4.5.3 Kontrola dokumentacji);
  - (e) program szkoleń jest regularnie poddawany przeglądowi i audytowi (zob. pkt 6.2. Audyt wewnętrzny), a w sytuacjach, gdy jest to konieczne, wprowadzane są w nim zmiany (zob. pkt 5.4 Zarządzanie zmianą).
- 4.2.3. Dla pracowników wprowadzono mechanizmy „powrotu do pracy” po wypadkach, incydentach lub długotrwałej nieobecności w pracy, obejmujące zapewnienie dodatkowych szkoleń w przypadku stwierdzenia takiej potrzeby.

### 4.2.2 Cel

Celem tego wymogu jest zapewnienie, aby organizacja posiadała stosowne struktury i zasoby mające na celu kontrolowanie napotykanego ryzyka, oraz umożliwienie jej rozmieszczania personelu, który jest w stanie należycie pełnić powierzone mu funkcje związane z bezpieczeństwem, w szczególności te o kluczowym znaczeniu dla bezpieczeństwa. System zarządzania kompetencjami zapewni również organizacji możliwość utrzymania umiejętności, wiedzy i doświadczenia personelu w długim okresie.

Kompetencja odgrywa kluczową rolę w zapewnieniu odpowiedniego sposobu podejmowania działań. Wymóg dotyczący konieczności dysponowania kompetentnymi pracownikami dotyczy nie tylko pracowników działających na pierwszej linii (w tym wykonawców, konsultantów i dostawców usług związanych z bezpieczeństwem), ale również kadry kierowniczej. Wymogi dotyczące kompetencji kadry kierowniczej są często pomijane; pracownicy pełniące funkcje kierownicze podejmują jednak istotne decyzje, które mogą mieć poważne i dalekosiężne skutki dla zdrowia i bezpieczeństwa. Wspomniane wymogi powinny obejmować postanowienia dotyczące szkolenia wszystkich pracowników w zakresie obowiązujących norm bezpieczeństwa; postanowienia dotyczące utrzymywania kompetencji niezależnie od okoliczności, w tym niezależnie od kwestii takich jak dostępność pracowników; oraz postanowienia dotyczące monitorowania poziomów kompetencji w odniesieniu do wymaganych norm.

W tym kontekście bezpieczeństwo postrzega się jako nieodzowny element profesjonalnego zachowania i profesjonalizmu, a nie jako „dodatkową płaszczyznę” stanowiącą uzupełnienie umiejętności zawodowych. Ponadto zdolność danej organizacji do radzenia sobie z nieprzewidzianymi zdarzeniami w czasie rzeczywistym zależy w dużym stopniu od kompetencji pracowników pierwszego kontaktu i osób sprawujących nad nimi nadzór. Kompetencje te można rozwijać, np. w ramach symulacji i regularnych szkoleń obejmujących złożone scenariusze.

#### 4.2.3 Noty wyjaśniające

Program szkoleniowy **(4.2.2)** może zostać przeprowadzony przez zewnętrzny ośrodek szkoleniowy. W takim przypadku organizacja powinna zapewnić, aby ośrodek szkoleniowy posiadał kompetencje do świadczenia stosownych usług – np. posiada certyfikację lub został uznany w systemie krajowym lub europejskim albo poprzez bezpośrednie monitorowanie działalności szkoleniowej i jej wyników. Ośrodki szkoleniowe mogą zaspokajać wszystkie potrzeby organizacji związane ze szkoleniami lub tylko niektóre z nich, w zależności od kompetencji, które ośrodki mają w poszczególnych dziedzinach. W przypadku gdy zewnętrzny ośrodek szkoleniowy zapewnia organizacji szkolenia, organizacja musi sprawdzić, czy szkolenie obejmuje niezbędne elementy, a jeśli nie, to w razie potrzeby, uzupełniać takie zewnętrzne szkolenie wewnętrznym szkoleniem.

#### **Jak uwzględnić czynniki ludzkie i organizacyjne oraz kulturę bezpieczeństwa?**

Kompetencje są integralną częścią systemu zarządzania kompetencjami i obejmują umiejętności pozatechniczne, postawy i zachowania. Określono niezbędne poziomy wymaganych kompetencji do wykonania zadania i przedstawiono związek z oceną ryzyka i analizami zadań.

„Postawa” **[4.2.1 lit. a)]** jest wykorzystywana do opisu sposobu, w jaki ludzie reagują na różne sytuacje, i jak się ogólnie zachowują (np. czy są proaktywni, czy są w stanie budować pozytywne relacje z innymi ludźmi). Jest to bardzo ważne w odniesieniu do tworzenia wzajemnych powiązań w ramach działalności związanej z systemem zarządzania bezpieczeństwem.

Istnieje systematyczne podejście zapewniające dostęp do kompetencji w zakresie czynników ludzkich i organizacyjnych w ramach właściwych ról w oparciu o ocenę ryzyka i analizy zadań.

Kompetencje w zakresie czynników ludzkich i organizacyjnych mogą być na przykład wykorzystywane w ocenie ryzyka, w projektach związanych z nowymi lub zmienionymi koncepcjami, w ramach oceny i poprawy wyników – aby zapewnić pozatechniczną perspektywę – lub w odniesieniu do kwestii związanych z działaniami człowieka. Szczegółowe szkolenia z zakresu czynników ludzkich i organizacyjnych, mające na celu zwiększenie świadomości, są prowadzone dla kadry kierowniczej i pracowników wykonujących zadania związane z bezpieczeństwem.

#### 4.2.4 Dowody

- Wnioskodawca powinien dostarczyć informacje na temat swojego systemu zarządzania kompetencjami i sposobu jego działania w kwestii wypełniania warunków przedstawionych w wymogach; **(4.2.1), [4.2.2 lit. a)–e])**
- dowody zawierają informacje szczegółowe na temat programów szkoleniowych, do których dostęp mają pracownicy (w tym w razie potrzeby wymogi dotyczące kompetencji osób prowadzących szkolenia), oraz tego, jak zapewnia się, że szkolenia są aktualne i jak dokonuje się ich przeglądu (w tym, w razie potrzeby, w odniesieniu do roli doradcy ds. bezpieczeństwa w ramach regulaminu RID lub, *w stosownych przypadkach, w odniesieniu do kompetencji pracowników odpowiedzialnych za utrzymanie zgodnie z wymogami załącznika I i załącznika II do rozporządzenia (UE) 2019/779 w sprawie podmiotów odpowiedzialnych za utrzymanie*); **[4.2.2 lit. a)–e])**
- dowody zawierają informacje na temat mechanizmów „powrotu do pracy” stosowanych wobec pracowników w następstwie wypadków, incydentów lub długiej nieobecności w pracy – w tym sposób, w jaki rozpoznaje się, czy są potrzebne dodatkowe szkolenia; **(4.2.3)**
- jeżeli wnioskodawca korzysta z usług uznanego ośrodka szkoleniowego certyfikowanego zgodnie z rozporządzeniami UE, kopia stosownego certyfikatu będzie dawała podstawy do domniemywania zgodności z powyższymi kryteriami w zakresie, w jakim zostały one objęte stosownym procesem certyfikacji; **[4.2.1 lit. a), c)–f]), (4.2.2)**
- wnioskodawca powinien wskazać, w jaki sposób zapewnia, aby kompetencje jego personelu oraz kompetencje wszystkich wykonawców, dostawców i konsultantów, z usług których korzysta, były takie same; **[4.2.1 lit. a)–f])**
- odpowiednie szkolenia z zakresu czynników ludzkich i organizacyjnych oraz zwiększania świadomości są prowadzone dla kadry kierowniczej i pracowników wykonujących zadania związane z bezpieczeństwem; **(4.2.1), (4.2.2)**
- wnioskodawca powinien wskazać, w jaki sposób oceniane są potrzeby dotyczące kompetencji w zakresie czynników ludzkich i organizacyjnych, co uwzględnia określanie, w jakich rolach i w jakich procesach istnieje zapotrzebowanie na kompetencje w zakresie czynników ludzkich i organizacyjnych oraz jaki poziom kompetencji jest wymagany. Dostępność czynnika ludzkiego (np. formalne kwalifikacje czynnika ludzkiego, tj. wykształcenie wyższe, wewnątrznie i zewnątrznie uznawane kompetencje i doświadczenie) jest dostosowana do dojrzałości i złożoności przedsiębiorstwa i proporcjonalna ich względem; **[4.2.1 lit. a)–f])**
- wnioskodawca powinien przedstawić opis procesu wydawania upoważnień dla personelu, który pełni kluczowe role, jak również bieżącego zarządzania kompetencjami personelu **(4.2.1 lit. a)–f), 4.2.2 lit. d).**

#### 4.2.5 Przykłady dowodów

System zarządzania kompetencjami wraz z wyjaśnieniem, w jaki sposób funkcjonuje w długim okresie – w tym, w stosownych przypadkach, w odniesieniu do pracowników, którzy nie wykonują funkcji pierwszoplanowych – a także wraz z odniesieniami do dokumentacji, która go uzasadnia, w tym do informacji dotyczących poszczególnych programów szkoleniowych i sposobu zarządzania ośrodkami szkoleniowymi, którym zlecono podwykonawstwo.

Wszelkie ustalenia umowne (w tym zakres zadań) zawarte z certyfikowanymi ośrodkami szkoleniowymi, wraz z dowodami potwierdzającymi ich certyfikację są dostarczone.

Przykłady programów szkoleniowych dla grup pracowników.

Uwzględnienie czynników ludzkich i organizacyjnych oraz poprawa kultury bezpieczeństwa będą miały pozytywny wpływ na spełnienie odpowiedniego wymogu systemu zarządzania bezpieczeństwem, a dowody na to można znaleźć w następujących źródłach:

Proces pokazujący, w jaki sposób zarządza się wymogami i kwalifikacjami, w tym dotyczącymi sprawności psychicznej lub fizycznej, uznanymi za niezbędne do pełnienia poszczególnych funkcji związanych z bezpieczeństwem, oraz w jaki sposób się ich przestrzega, w tym pokazujący związek z oceną ryzyka i analizami zadań.

Proces pokazujący, jak zarządza się wymogami i kwalifikacjami pracowników, zarówno w zakresie:

- *spełniania obowiązujących wymogów dotyczących sprawności fizycznej i psychicznej;*
- *określania kompetencji zawodowych uznanych za niezbędne do pełnienia poszczególnych funkcji związanych z bezpieczeństwem.*

Procesy okresowego przeglądu wymogów i programów szkoleniowych pokazują aktualną sytuację i są stale dostosowywane do zmian technicznych, operacyjnych i organizacyjnych.

Procedura lub proces zapewniające personelowi szkolenia specjalistyczne i odświeżające na wypadek następujących sytuacji:

- *planowanych zmian mających wpływ na przepisy wewnętrzne, infrastrukturę, strukturę organizacyjną itp.;*
- *aktualizacji zleconych zadań (np. w przypadku maszynistów, nowych tras, nowych rodzajów lokomotyw, nowych rodzajów usług).*

System zarządzania bezpieczeństwem opisujący, w jaki sposób zidentyfikowano i wdrożono potrzeby szkoleniowe w zakresie zadań związanych z bezpieczeństwem, zgodnie z określonymi funkcjami. Informacje dotyczące procesu są wykorzystywane do tworzenia materiałów szkoleniowych, a przepisy gwarantują, że zaangażowani pracownicy zapoznają się z ryzykiem związanym z ich działalnością.

Postępowanie wyjaśniające w sprawie wypadku i incydentu w zakresie, który dotyczy działań mających na celu modyfikację programów szkoleniowych w świetle wypadków i incydentów, przeprowadzonych działań nadzorczych itp.

Proces umożliwiający pracownikom kwestionowanie procedur i decyzji oraz zgłaszanie rutynowych i nietypowych odchyleń.

System zarządzania bezpieczeństwem opisujący, jakie mechanizmy dzielenia się wiedzą są dostępne w organizacji.

Proces mający na celu zapewnienie:

- *utrzymywania kompetencji poprzez wystarczające doświadczenie praktyczne w danej dziedzinie (np. w przypadku maszynistów wiedzy dotyczącej warunków prowadzenia działalności, kategorii pociągów, pojazdów trakcyjnych, linii i stacji) lub poprzez planowanie specjalistycznych szkoleń, w szczególności w przypadku długotrwałej nieobecności w pracy (np. choroby) lub wypadku/incydentu;*
- *okresowej oceny kompetencji w celu zapewnienia utrzymania nabytych kompetencji;*
- *podjęcia niezbędnego działania, w przypadku gdy zidentyfikowano przypadki braku zgodności z wymogami lub nieodpowiednich zachowań, takich jak wycofanie na pewien czas osoby lub sprzętu z użycia, ograniczenia dotyczące uznanych umiejętności, w przypadku gdy zidentyfikowano brak zgodności z wymogami, specjalistyczne szkolenia itp.;*
- *podjęcia odpowiednich środków w przypadku pracowników po wypadkach lub incydentach (np. w przypadku maszynistów, którzy zignorowali sygnał ostrzegawczy, wypadku z udziałem człowieka itp. Na przykład organizacja zapewnia gotowość maszynisty do ponownego podjęcia pracy lub możliwość zastąpienia go osobą kompetentną do świadczenia usługi);*

- *wymiany doświadczeń zyskanych w wyniku poważnych wypadków lub wszelkich innych znaczących zdarzeń, w szczególności gdy wykryto nowe ryzyko i istnieje konieczność zarządzania nim na poziomie operacyjnym;*
- *istnienia procedur monitorowania dla systemu zarządzania kompetencjami, w tym sposobu mierzenia jego skuteczności.*

System zarządzania bezpieczeństwem wyjaśniający, w jaki sposób kadra kierownicza jest szkolona, aby mogła przeprowadzać oceny ryzyka przed podjęciem decyzji, uwzględnia czynniki ludzkie i organizacyjne w swoich codziennych działaniach (ocena ryzyka, ocena wyników, doskonalenie...).

Proces zapewnienia ciągłości działania oraz proces dotyczący mechanizmów „powrotu do pracy” wraz z systemem zarządzania kompetencjami.

Program szkoleniowy pokazujący, że określone metody szkoleniowe określa się zgodnie z celami i kryteriami szkolenia:

- *mentoring;*
- *szkolenia w miejscu pracy;*
- *symulatory;*
- *szkolenia na wypadek awarii;*
- *szkolenia zespołu z zakresu zarządzania zasobami.*

Proces zapewnienia personelowi odpowiednich kompetencji, w tym określenie niezbędnych kompetencji, jest powiązany z oceną ryzyka. Wprowadzony proces pokazuje, że istnieje usystematyzowane podejście wykorzystujące kompetencje w zakresie czynników ludzkich i organizacyjnych dla personelu przeprowadzającego ocenę ryzyka i określającego wynikające z tego funkcje i kompetencje w zakresie bezpieczeństwa, aby zapewnić przydzielenie niezbędnych zasobów i kompetencji.

Kompetencja w zakresie kultury bezpieczeństwa opierająca się na analizie potrzeb. Ocenia się potrzeby dotyczące kompetencji w zakresie kultury bezpieczeństwa oraz wskazuje strategie mające zapewnić właściwe kompetencje i zasoby. Wykazano, że podstawowa wiedza na temat kultury bezpieczeństwa i jej znaczenie są promowane przez zarząd.

Proces zapewniający, by wykonawcy, partnerzy i dostawcy spełniali te same wymagania dotyczące kompetencji. Ustalenia umowne (lub umowy partnerskie) odnoszące się do tych wymogów oraz monitorowanie wykonania umowy (lub partnerstwa).

#### 4.2.6 Odniesienia i normy

- *ISO10015:2019 „Wytyczne dotyczące zarządzania jakością w zakresie zarządzania kompetencjami i rozwoju ludzi”*
- *ISO10018:2020 „Zarządzanie jakością – Wytyczne dotyczące zarządzania ludźmi”*

#### 4.2.7 Kwestie związane z nadzorem

W jaki sposób wyniki oceny ryzyka łączą się z przeglądem systemu zarządzania kompetencjami.

Przy przeprowadzaniu analizy systemu zarządzania kompetencjami należy pamiętać o tym, że niektóre wymagania w zakresie kompetencji obejmują nie tylko pracowników danej organizacji, ale wywierają również wpływ na wykonawców i inne podmioty.

Należy kontrolować system zarządzania kompetencjami, aby sprawdzić, w jakim stopniu jest on aktualny i czy działania szkoleniowe podjęte w ramach tego systemu odpowiadają obecnym potrzebom organizacji.

Organizacja powinna posiadać określone środki zapewniające kompetencję personelu przeprowadzającego działania. Jest to szczególnie ważne w przypadku wykonawców, którym zlecono wykonanie wyłącznie ściśle określonych prac, ponieważ kontrole kompetencji przeprowadzane w odniesieniu do takich wykonawców nie muszą być aż tak szczegółowe.

Poziom kompetencji w przypadku wykonywania podobnych działań powinien być taki sam między personelem zatrudnionym bezpośrednio i wykonawcami.

Istnieje system zapewniający identyfikację zadań i stanowisk zawierających element bezpieczeństwa, w tym czynności o istotnym znaczeniu dla bezpieczeństwa.

Istnieje solidny i skuteczny system zarządzania kompetencjami obejmujący: określanie niezbędnej wiedzy i umiejętności, szkolenie, utrzymanie poziomu kompetencji i zasoby w zakresie kompetencji; proces rekrutacji, szkolenia, oceny monitorowania kompetencji i proces prowadzenia rejestrów, wskazujący w jaki sposób wszystkie te czynniki przyczyniają się do osiągnięcia i utrzymania poziomu kompetencji.

Koncentracja na czynnikach ludzkich – w jaki sposób organizacja dokonuje oceny sprawności fizycznej i psychicznej (np. maszynistów i innych pracowników wykonujących czynności o istotnym znaczeniu dla bezpieczeństwa).

## 4.3 Świadomość

### 4.3.1 Wymóg regulacyjny

4.3.1. Kadra kierownicza wyższego szczebla musi zapewnić, by zarówno jej członkowie, jak i pracownicy pełniący funkcje mające wpływ na bezpieczeństwo mieli świadomość znaczenia, wagi i konsekwencji swoich działań oraz tego, w jaki sposób przyczyniają się one do prawidłowego stosowania i skuteczności systemu zarządzania bezpieczeństwem, w tym do osiągnięcia celów w zakresie bezpieczeństwa (zob. pkt 3.2 Cele w zakresie bezpieczeństwa i planowanie).

### 4.3.2 Cel

Świadomość oznacza podnoszenie wiedzy pracowników na temat strategii organizacji w zakresie bezpieczeństwa i tego, w jaki sposób pracownicy przyczyniają się do zapewnienia bezpieczeństwa w organizacji, wiedzy na temat zagrożeń i ryzyk, których pracownicy muszą być świadomi, oraz wyników dochodzeń w sprawie wypadków i incydentów. Oznacza ona również świadomość konsekwencji nieuczestniczenia we wdrażaniu systemu zarządzania bezpieczeństwem zarówno dla samego pracownika, jak i organizacji. Celem tego wymogu jest rozwiązanie kwestii związanych z kulturą bezpieczeństwa w ramach organizacji. To kadra kierownicza wyższego szczebla ustala plan działania i ukierunkowanie organizacji oraz określa sposób prowadzenia działalności. Personel działający w ramach organizacji weźmie przykład z kierownictwa. Wnioskodawca będzie musiał wykazać, w jaki sposób rozwiązuje się takie kwestie w ramach procesów i procedur w jego organizacji.

### 4.3.3 Noty wyjaśniające

Wymóg ten związany jest z czynnikami ludzkimi i organizacyjnymi. Dodatkowe informacje dotyczące czynników ludzkich i organizacyjnych można znaleźć w załączniku 5.

### 4.3.4 Dowody

- *Wnioskodawca powinien wskazać miejsce, w którym w ramach jego zasobów ludzkich lub innych procesów znajduje odzwierciedlenie kluczowa rola, którą pracownicy odgrywają w realizacji celów organizacji, w jaki sposób stara się to oszacować i jakie kroki podejmuje w celu utrzymania i poprawy istniejącego stanu; (4.3.1) (zob. również 2.3)*
- *informacje na temat funkcjonowania systemu zarządzania kompetencjami. (4.3.1)*

### 4.3.5 Przykłady dowodów

Uwzględnienie czynników ludzkich i organizacyjnych oraz poprawa kultury bezpieczeństwa będą miały pozytywny wpływ na spełnienie odpowiedniego wymogu systemu zarządzania bezpieczeństwem, a dowody na to można znaleźć w następujących źródłach:

Deklaracja zawarta w strategii w zakresie bezpieczeństwa lub w innym miejscu dotycząca zaangażowania „zarządzających umysłów” organizacji w promowanie kultury bezpieczeństwa organizacji w celu zapewnienia kontroli ryzyka poprzez podejście oparte na systemie zarządzania. Dokument wskaże również rolę wszystkich pracowników w promowaniu strategii w zakresie bezpieczeństwa – poprzez osiąganie określonych celów w zakresie bezpieczeństwa. Zapewniono powiązania ze szczególnymi procedurami mającymi na celu promowanie tych założeń w całej organizacji.

Proces monitorowania obejmuje element dotyczący zrozumienia w całej organizacji systemu zarządzania bezpieczeństwem oraz znaczenia i świadomości ryzyka poszczególnych zadań.

Regularne przeprowadzanie badań zaangażowania pracowników z naciskiem na bezpieczeństwo, które pokazują, że pracownicy rozumieją, jak ich rola wpisuje się w ogólne cele organizacji w zakresie bezpieczeństwa.

Programy szkoleniowe zawierające wyjaśnienia dotyczące zagrożeń, środków bezpieczeństwa i celów w zakresie bezpieczeństwa przy wykonywaniu zadań i podzadań.

W procedurze, którą mogą stosować pracownicy, wykonawcy lub inne zainteresowane strony, aby zgłosić ryzyko, na które są narażeni.

Deklaracja obejmująca wskazanie sposobu, w jaki organizacja zachęca swoich wykonawców, partnerów i dostawców do przyjęcia jej podejścia do zwiększania świadomości w zakresie bezpieczeństwa, czynników ludzkich i organizacyjnych oraz kultury bezpieczeństwa.

W powiadomieniach o celach od kadry kierowniczej wyższego szczebla, aby zachęcić wszystkich pracowników do udziału w ich osiągnięciu albo na przykład pogratulować poprawy skuteczności działania.

W informacji wskazującej, że kierownictwo średniego szczebla i personel operacyjny są zaangażowani w pierwszoplanowe inicjatywy na rzecz bezpieczeństwa (warsztaty, fora, dni poświęcone bezpieczeństwu, programy szkoleń ukierunkowane na podnoszenie świadomości w zakresie ich roli w ramach systemu zarządzania bezpieczeństwem itp.).

Opis kanałów komunikacyjnych i zastosowanych kanałów oraz sposobów włączenia czynników ludzkich i organizacyjnych.

W procesie projektowania procedur wyjaśniającym, w jaki sposób zaangażowany jest zainteresowany personel oraz w jaki sposób uwzględnia się ryzyko i środki bezpieczeństwa, a także potencjalny wpływ braku zgodności na działania operacyjne.

#### 4.3.6 *Kwestie związane z nadzorem*

Podczas przeprowadzania rozmów z pracownikami na temat tej kwestii ważne jest, aby ustalić charakter zrozumienia, które ludzie posiadają w zakresie ról i obowiązków, które ich dotyczą. Ustalenie tego wskaże, czy organizacja jest w stanie zrozumieć znaczenie skutecznej kultury organizacyjnej lub świadomości w zapewnianiu bezpieczeństwa poprzez system zarządzania bezpieczeństwem.

Główne pytania w zakresie nadzoru to: na jakiej podstawie organizacja oparła swoją obecną kulturę i jakie kroki podjęła w celu jej poprawy i rozwoju.

Kontrola monitorowania w zakresie wypełniania obowiązków/celów dotyczących zdrowia i bezpieczeństwa, świadomości zagrożenia, kultury sprawozdawczej – wyszukiwanie pomyłek, błędów, przypadków naruszeń i innych nieprawidłowości.



## 4.4 Informowanie i komunikowanie

### 4.4.1 Wymóg regulacyjny

|   |
|---|
| <p>4.4.1. Organizacja musi określić odpowiednie kanały komunikacji w celu zapewnienia, by informacje dotyczące bezpieczeństwa były wymieniane między różnymi szczeblami organizacji oraz z zewnętrznymi zainteresowanymi stronami, w tym wykonawcami, partnerami i dostawcami.</p> <p>4.4.2. Aby zapewnić, by informacje dotyczące bezpieczeństwa docierały do osób dokonujących osądów i podejmujących decyzje, organizacja musi zarządzać identyfikowaniem, otrzymywaniem, przetwarzaniem, generowaniem i rozpowszechnianiem informacji dotyczących bezpieczeństwa.</p> <p>4.4.3. Organizacja musi zapewnić, by informacje dotyczące bezpieczeństwa były:</p> <ul style="list-style-type: none"><li>(a) istotne, pełne oraz możliwe do zrozumienia przez docelowych użytkowników;</li><li>(b) aktualne;</li><li>(c) dokładne;</li><li>(d) spójne;</li><li>(e) skontrolowane (zob. Kontrola dokumentacji);</li><li>(f) upowszechnione przed rozpoczęciem ich obowiązywania;</li><li>(g) odebrane i zrozumiane.</li></ul> |
|---|

### 4.4.2 Cel

Powyższe wymagania opracowano, aby wnioskodawca wykazał we wniosku, iż posiada właściwe środki do zidentyfikowania, na różnych poziomach, informacji dotyczących bezpieczeństwa i przekazania ich we właściwym czasie właściwym osobom. Wnioskodawca powinien identyfikować otoczenie systemu w celu zapewnienia, aby obecne środki kontroli ryzyka były adekwatne i aktualne oraz aby organizacja była w stanie identyfikować nowe zagrożenia i szanse wynikające z wpływów zewnętrznych (tj. polityczne, społeczne, środowiskowe, technologiczne, gospodarcze i prawne). Wnioskodawca jest w stanie uzyskać pewność, że dociera w swojej organizacji do właściwych pracowników (w szczególności do pracowników na stanowiskach o istotnym znaczeniu dla bezpieczeństwa), których reakcja na to jest wymagana. Będzie to uwzględniać sposób, w jaki przekazują istotne informacje związane z bezpieczeństwem innym zainteresowanym stronom, z którymi współpracują.

### 4.4.3 Noty wyjaśniające

Organizacja precyzuje, jaki rodzaj informacji związanych z bezpieczeństwem trzeba przekazać, w jaki sposób zostaną przekazane (**zob. również 4.5**), do kogo i na podstawie jakich warunków zostanie ta czynność rozpoczęta i przeprowadzona (**4.4.1**). Wymiana informacji związanych z bezpieczeństwem odbywa się między pracownikami organizacji i podwykonawcami, partnerami lub dostawcami; między przedsiębiorstwami kolejowymi i zarządcami infrastruktury oraz tam gdzie jest to stosowne, między zarządcami infrastruktury.

Można wyróżnić różne rodzaje informacji:

- *dokumentacja systemu zarządzania bezpieczeństwem (**zob. również 4.5**);*
- *standardowe informacje wymagane od zarządcy infrastruktury w celu zaplanowania przewozów, takie jak przepisy operacyjne i charakterystyka infrastruktury kolejowej (np. szerokość toru, dopuszczalna długość pociągu, pochYLENIE toru i nacisk osiowy);*

- *informacje konieczne do zaplanowania przewozów, takie jak: harmonogramy pracy stacji, wykaz tras, tymczasowe ograniczenia prędkości, zmiany w infrastrukturze kolejowej, trwające prace na torach, ograniczenia szerokości toru, pociągi przekierowane z normalnej trasy, linie eksploatowane jednotorowo, rozkład jazdy pociągów (w tym wszelkie zmiany tras pociągów lub przewozów podmiejskich);*
- *informacje dotyczące zarządzania ruchem kolejowym (między przedsiębiorstwami kolejowymi i zarządcami infrastruktury; oraz – w stosownych przypadkach – między zarządcami infrastruktury), w tym wskazanie w każdej organizacji kompetentnych pracowników, z którymi można się skontaktować w sytuacji awarii lub w sytuacjach kryzysowych (**zob. również 5.5**), zarówno w czasie głównych godzin pracy, jak i poza nimi.*

Podstawowe wymogi dotyczące wymiany informacji (**4.4.2**) między przedsiębiorstwem kolejowym i zarządcą infrastruktury są określone w TSI OPE. W rozporządzeniu w sprawie podmiotów odpowiedzialnych za utrzymanie – między przedsiębiorstwem kolejowym i podmiotem odpowiedzialnym za utrzymanie, we wspólnej metodzie oceny bezpieczeństwa w odniesieniu do wymogów dotyczących systemu zarządzania bezpieczeństwem – między przedsiębiorstwem kolejowym/zarządcą infrastruktury i organami (Agencją, krajowym organem ds. bezpieczeństwa).

Istnieją również ustalenia dotyczące wymiany informacji z odpowiednimi stronami w odniesieniu do zagrożeń wynikających z wad, niezgodności konstrukcyjnych lub wadliwego działania systemów technicznych, w tym podsystemów strukturalnych oraz informacji o wszelkich działaniach naprawczych. Do wymiany informacji może służyć np. system SAIT (Safety Alert Tool), który był promowany przez Agencję w sektorze kolejowym. Stosowanie SAIT spełnia obowiązek określony w dyrektywie w sprawie bezpieczeństwa kolei (art. 4 ust. 5) oraz wymóg w CSM w sprawie monitorowania (art. 4) oraz w rozporządzeniu w sprawie podmiotów odpowiedzialnych za utrzymanie (art. 5 ust. 5 w zakresie wymiany informacji).

„Aktualne” w powyższym kontekście [**4.4.3 lit. b**] oznacza aktualne.

„Spójne” w powyższym kontekście [**4.4.3 lit. d**] oznacza brak konfliktów, w przypadku pochodzenia z różnych źródeł.

„Zrozumiane” w powyższym kontekście [**4.4.3 lit. g**] oznacza, że wnioskodawca wykazał, iż działania mające na celu zapewnienie, aby informacje o istotnym znaczeniu dla bezpieczeństwa zostały przyjęte przez tych, do których są adresowane. Można to osiągnąć za pomocą szkoleń ad hoc, pytań sprawdzających prawidłowe zrozumienie na odprawach lub – w komunikacji o istotnym znaczeniu dla bezpieczeństwa – poprzez przyjęcie uregulowań, które wymagają, aby istotne wiadomości były powtarzane, np. między dyżurnym ruchu a maszynistą w celu potwierdzenia, że wiadomości zostały poprawnie zrozumiane, lub za pomocą dowolnych środków, które spełniają ten wymóg.

Wymóg ten związany jest z czynnikami ludzkimi i organizacyjnymi. Więcej informacji dotyczących czynników ludzkich i organizacyjnych można znaleźć w części Załącznik 5.

#### 4.4.4 Dowody

- *Wnioskodawca wskazuje różne kanały komunikacji, które istnieją w organizacji oraz ich cel; (**4.4.1**)*
- *wnioskodawca musi dostarczyć dowody na przykład na temat jakiegokolwiek wewnętrznego systemu powiadamiania o bezpieczeństwie; jakiegokolwiek systemu dostarczającego pracownikom istotnych, chociaż rutynowych, informacji; oraz jakiegokolwiek systemu dostarczającego pracownikom istotnych informacji, które mają charakter ad hoc; (**4.4.2**)*
- *wnioskodawca wskazuje sposób, w jaki upewnia się, że informacje, które rozprawdzono, dotarły do tych, do których miały dotrzeć (szczególnie w odniesieniu do osób, których rola ma istotne znaczenie dla bezpieczeństwa) oraz że zostały przez nich zrozumiane. (**4.4.3**)*

#### 4.4.5 Przykłady dowodów

Proces lub procedura, który/-a pozwala się upewnić, że strony zewnętrzne takie jak zarządca lub zarządcy infrastruktury, (inne) przedsiębiorstwa kolejowe, organy itp. mają kontakt z kimś, kto jest w stanie się z nimi porozumieć (np. posiada umiejętności językowe) i ma dostęp do odpowiednich informacji.

Proces lub procedura dotyczące potwierdzania dostarczenia dokumentów związanych z bezpieczeństwem.

W odniesieniu do ról, którym powierzono zarządzanie powiązaniem: dowody wskazujące do kogo alarm bezpieczeństwa jest wysyłany w zależności od obszaru działalności (np. alerty bezpieczeństwa są zawarte w opisie trasy lub informacjach o ostatnich zmianach),

Uwzględnienie czynników ludzkich i organizacyjnych oraz poprawa kultury bezpieczeństwa będą miały pozytywny wpływ na spełnienie odpowiedniego wymogu systemu zarządzania bezpieczeństwem, a dowody na to można znaleźć w następujących źródłach:

W jasnej deklaracji dotyczącej sposobu, w jaki funkcjonuje komunikacja zarówno w górę, jak i w dół, w odniesieniu do różnych rodzajów i poziomów informacji – w tym odniesienia do konkretnych procedur dotyczących alarmów bezpieczeństwa i rutynowej komunikacji.

W procesie lub procedurze, w której wskazuje się, jakie podejmowane są działania w odniesieniu do różnych rodzajów wiadomości w celu zapewnienia, aby dotarły do pracowników, do których mają dotrzeć, i że ci pracownicy rozumieją przekaz np. informacje o istotnym znaczeniu dla bezpieczeństwa.

Proces lub procedura, które zapewniają, że każdy pracownik zaangażowany w zadanie związane z bezpieczeństwem otrzymuje właściwą wersję dokumentów we właściwym czasie, aby zapewnić zaangażowanie i zdolność do szybkiego działania lub reagowania w sytuacjach normalnych, awaryjnych i kryzysowych.

TSI OPE zawiera wymogi dotyczące różnych dokumentów, w tym niektóre odnoszące się do komunikacji pomiędzy personelem przedsiębiorstw kolejowych a zarządcami infrastruktury. Istnieje świadomość, że wszystkie te dokumenty (regulamin, księga tras, rozkłady jazdy, księgi formularzy...) zawierają zestaw protokołów komunikacyjnych lub mediów dotyczących jasnej i sprawnej wymiany sformalizowanych informacji mających wpływ na działalność, w szczególności na ruch pociągów w trybie awaryjnym.

Alarmy bezpieczeństwa, którymi należy wymieniać się wewnątrz organizacji lub z innymi zainteresowanymi stronami. Przykłady niektórych typowych sytuacji:

- *Przedsiębiorstwo kolejowe dostarcza informacje zarządcy infrastruktury dotyczące wszelkich zdarzeń, które mogą wpłynąć na ruch pociągów (problemów z taborem kolejowym, np. zagrane łożyska osiowe, dzięki czemu zarządca infrastruktury może podjąć działania mające na celu kontrolę ryzyka takie jak zamknięcie ruchu na torze obok).*
- *Zarządca infrastruktury dostarcza informacje na temat problemów z infrastrukturą i tymczasowych środków bezpieczeństwa, które zostaną zastosowane, takich jak ograniczenie prędkości obowiązujące wszystkie przedsiębiorstwa kolejowe, które prowadzą działalność na danym obszarze.*

Proces lub procedura dotyczące rozpowszechniania informacji na temat zmian w strukturze organizacyjnej organizacji, zarówno na poziomie mikro, jak i makro.

Kopie instrukcji wydanych pracownikom wykonującym zadania związane z bezpieczeństwem, w których odnosi się do zasad funkcjonowania dotyczących sieci i które są:

- *kompletne: wszystkie przepisy i wymogi istotne dla zadań dotyczących kwestii bezpieczeństwa, które są związane z działalnością przedsiębiorstwa kolejowego, są wskazane i przepisane do stosownych dokumentów;*

- *dokładne: wszystkie przepisy i wymogi są poprawnie i bezbłędnie przepisane (np. co należy robić przed rozpoczęciem komunikacji związanej z sygnałem lub bezpieczeństwem);*
- *spójne: pochodzące z różnych źródeł wymogi stosowane wobec pojedynczej osoby lub pojedynczego zespołu są wzajemnie zgodne i spójne i nie występują między nimi konflikty.*

Proces rejestrowania informacji jest ustalony w odpowiednich przepisach wewnętrznych, z wykorzystaniem odpowiedniego kanału komunikacji.

W programach szkoleniowych określa się sposób zarządzania komunikacją i w jaki sposób umiejętności komunikacyjne są zintegrowane z systemem zarządzania kompetencjami.

Proces sprawozdawczy umożliwiający pracownikom zgłaszanie kwestii związanych z bezpieczeństwem w ramach polityki *just culture* wyjaśnia, w jaki sposób te informacje zwrotne są analizowane i oceniane, tak aby ukryte błędy systemu mogły być dostrzeżone i uwzględnione w procesie zarządzania ryzykiem. Proces obejmuje również sposób przekazywania pracownikom informacji zwrotnych dotyczących przedkładania sprawozdań.

Procedura wyjaśniająca różne rodzaje spotkań i odpowiednie wyniki (np. protokoły spotkań, notatki, ...) pokazuje, w jaki sposób zarządza się komunikacją w zakresie bezpieczeństwa zarówno w górę, jak i w dół przedsiębiorstwa.

#### 4.4.6 Kwestie związane z nadzorem

Należy sprawdzić, czy stosowane są techniki i procesy mające na celu zapewnienie bycia na bieżąco w kwestii kontroli ryzyka, wypatrywania odległych możliwości i zagrożeń.

Należy sprawdzić, czy istnieje proces mający na celu monitorowanie wykorzystania sformalizowanych informacji.

Kluczowymi kwestiami z punktu widzenia nadzoru jest to, jak aktualne są informacje i czy odpowiednio szybko docierają do **wszystkich** pracowników, do których mają dotrzeć, np. do tych na nocnej zmianie lub tych którzy pracują zdalnie z głównych jednostek organizacji.

## 4.5 Dokumentacja

### 4.5.1 Wymóg regulacyjny

#### 4.5.1. Dokumentacja systemu zarządzania bezpieczeństwem

##### 4.5.1.1. Istnieje opis systemu zarządzania bezpieczeństwem obejmujący:

- (a) wskazanie i opis procesów i działań związanych z bezpieczeństwem działalności kolejowej, w tym zadań związanych z bezpieczeństwem oraz związanej z nimi odpowiedzialności (zob. pkt 2.3 Funkcje, odpowiedzialność, rozliczalność i uprawnienia w ramach organizacji);
- (b) interakcje między tymi procesami;
- (c) procedury lub inne dokumenty opisujące sposób wdrożenia tych procesów;
- (d) wskazanie wykonawców, partnerów i dostawców wraz z opisem rodzaju i zakresu świadczonych usług;
- (e) wskazanie ustaleń umownych oraz innych porozumień biznesowych, zawartych przez organizację z innymi stronami wskazanymi w lit. d), niezbędnych do kontroli ryzyk dla bezpieczeństwa, przed którymi stoi organizacja, oraz ryzyk związanych z korzystaniem z wykonawców;
- (f) odesłania do dokumentacji wymaganej na podstawie niniejszego rozporządzenia.

##### 4.5.1.2. Organizacja musi zapewnić złożenie rocznego sprawozdania dotyczącego bezpieczeństwa odpowiedniemu krajowemu organowi (lub odpowiednim krajowym organom) ds. bezpieczeństwa zgodnie z art. 9 ust. 6 dyrektywy (UE) 2016/798, obejmującego:

- (a) syntezę decyzji dotyczących poziomu znaczenia zmian związanych z bezpieczeństwem, w tym przegląd znaczących zmian, zgodnie z art. 18 ust. 1 rozporządzenia (UE) nr 402/2013;
- (b) cele organizacji w zakresie bezpieczeństwa na następny rok (następne lata) oraz określenie tego, w jaki sposób poważne ryzyka dla bezpieczeństwa wpływają na określenie tych celów w zakresie bezpieczeństwa;
- (c) wyniki wewnętrznych dochodzeń dotyczących wypadków lub incydentów (zob. pkt 7.1 Wyciąganie wniosków z wypadków i incydentów) oraz innych działań w zakresie monitorowania (zob. pkt 6.1 Monitorowanie, pkt 6.2 Audyt wewnętrzny i pkt 6.3 Przegląd dokonywany przez kierownictwo), zgodnie z art. 5 ust. 1 rozporządzenia (UE) nr 1078/2012;
- (d) szczegółowe informacje dotyczące postępów w zastosowaniu się do niezamkniętych zaleceń krajowych organów dochodzeniowych (zob. pkt 7.1 Wyciąganie wniosków z wypadków i incydentów);
- (e) wskaźniki bezpieczeństwa określone przez organizację na potrzeby oceny wyników organizacji w zakresie bezpieczeństwa (zob. pkt 6.1 Monitorowanie);
- (f) w stosownych przypadkach wnioski zawarte w rocznym sprawozdaniu doradcy ds. bezpieczeństwa, o którym mowa w RID, na temat działalności organizacji w odniesieniu do transportu towarów niebezpiecznych.

#### 4.5.2. Tworzenie i aktualizowanie

##### 4.5.2.1. Organizacja musi zapewnić, by w przypadku tworzenia i aktualizowania dokumentacji dotyczącej systemu zarządzania bezpieczeństwem stosowane były odpowiednie formaty i nośniki.

#### 4.5.3. Kontrola dokumentacji

4.5.3.1. Organizacja musi kontrolować dokumentację dotyczącą systemu zarządzania bezpieczeństwem, w szczególności jej przechowywanie, dystrybucję i kontrolę zmian, tak aby w stosownych przypadkach zapewnić jej dostępność, przydatność i ochronę.

#### 4.5.2 Cel

Wnioskodawca musi wykazać, że ogólny system zarządzania bezpieczeństwem jest odpowiedni dla rodzaju i zakresu świadczonych usług i jest w stanie zarządzać powstałym ryzykiem. Wymaga to:

- wyjaśnienia strategii wnioskodawcy w zakresie bezpieczeństwa, organizacji i uzgodnień na wysokim poziomie dotyczących systemu zarządzania bezpieczeństwem oraz
- bardziej szczegółowych ustaleń określonych w powyższych wymogach – pkt 4.5.1.1 lit. a)–f) i pkt 4.5.1.2 lit. a)–f).

Wnioskodawca musi również przedstawić sposób, w jaki zarządza się jego dokumentacją systemu zarządzania bezpieczeństwem, tj. identyfikacją, tworzeniem, utrzymaniem, zarządzaniem, przechowywaniem i zapisywaniem dokumentacji (tzn. dokumentów i zapisów/danych), aby zapewnić, że dokumentacja jest aktualna i odnośni pracownicy, w razie potrzeby, mają dostęp do poprawnych wersji.

#### 4.5.3 Noty wyjaśniające

Wszelkie dokumenty, w których wnioskodawca wykazuje zgodność swojego systemu zarządzania bezpieczeństwem z obowiązującymi wymogami [4.5.1.1 lit. f)] są częścią dokumentacji systemu zarządzania bezpieczeństwem.

Poniższy Rys. 3 przedstawia typową strukturę dokumentacji:



Rys. 3: Typowa struktura dokumentacji

W zależności od obszaru działalności przedsiębiorstwa kolejowe mogą złożyć różne sprawozdania (4.5.1.2) do krajowych organów ds. bezpieczeństwa państw członkowskich, w których prowadzą działalność. Zasadniczo zakres sprawozdania odnosi się jedynie do części działalności prowadzonej w odnośnym państwie

członkowskim. Agencja zaleca jednak, by to samo sprawozdanie obejmowało cały obszar działalności – co powinno usprawnić wymianę informacji między krajowymi organami ds. bezpieczeństwa nadzorującymi to samo przedsiębiorstwo kolejowe.

Roczne sprawozdanie doradcy ds. bezpieczeństwa [4.5.1.2 lit. f)], w przypadku transportu towarów niebezpiecznych, wymagane zgodnie ze zmienioną dyrektywą 2008/68/WE, z późniejszymi zmianami, i Regulaminem międzynarodowego przewozu kolejami towarów niebezpiecznych, roczne sprawozdanie doradcy ds. bezpieczeństwa ładunków niebezpiecznych jest również bodźcem do sporządzenia rocznego sprawozdania dotyczącego bezpieczeństwa. Od doradcy ds. bezpieczeństwa wymaga się wypełniania określonych funkcji, w tym doradzanie przedsiębiorstwu, które go powołało, w zakresie kwestii związanych ze zdrowiem, bezpieczeństwem i środowiskiem w związku z transportem ładunków niebezpiecznych oraz w zakresie przygotowywania niezbędnych sprawozdań.

Identyfikację, strukturę (np. język, wersję oprogramowania, grafiki) i formę (np. papierową, elektroniczną) wykorzystaną do tworzenia dokumentacji (4.5.2.1) pozostawia się w gestii organizacji. Nie musi mieć formy pisemnego podręcznika papierowego.

#### **Jak uwzględnić czynniki ludzkie i organizacyjne oraz kulturę bezpieczeństwa?**

Kontrola dokumentu (4.5.3.1) oznacza proces (lub procedurę) określający wewnętrzne kontrole, w szczególności przegląd i zatwierdzenie stosowności przed wydaniem i użytkowaniem, które to kontrole należy rozważyć i wdrożyć w przypadku informacji, które muszą być udokumentowane. Ma ona na celu zidentyfikowanie statusu aktualnych wersji dokumentów, aby uniemożliwić korzystanie z nieważnych lub nieaktualnych dokumentów. W szczególności zapewnia:

- *dostępność właściwych wydań stosownych dokumentów we wszystkich miejscach, w których prowadzi się działalność niezbędną do skutecznego funkcjonowania systemu zarządzania bezpieczeństwem;*
- *natychmiastowe usuwanie nieważnych lub nieaktualnych dokumentów z wszystkich punktów wydawania lub użytkowania, lub zapobieganie ich nieumyślnemu wykorzystaniu w inny sposób;*
- *właściwe identyfikowanie nieaktualnych dokumentów zachowanych do celów prawnych lub archiwalnych.*

#### **4.5.4 Dowody**

- *W stosownych przypadkach wnioskodawca powinien dostarczyć opis systemu zarządzania bezpieczeństwem i sposobu jego działania z właściwymi odesłaniami do odnośnych procedur; [4.5.1.1 lit. a)–c)]*
- *wnioskodawca powinien określić, kim są jego wykonawcy, dostawcy i partnerzy oraz w jaki sposób relacje te są kontrolowane i monitorowane, aby upewnić się, że ryzyka dla bezpieczeństwa zarówno ze strony wnioskodawcy, jak i podmiotów, z którymi łączą go relacje umowne, są odpowiednio zarządzane w celu zapewnienia bezpieczeństwa; [4.5.1.1 lit. d), e)]*
- *wnioskodawca powinien przedstawić odpowiednią procedurę lub procedury, które wykażą, że jest w stanie kontrolować udokumentowane informacje; [4.5.1.1 lit. f)]*
- *wnioskodawca powinien określić role i obowiązki, które mają zastosowanie w odniesieniu do zadań związanych z bezpieczeństwem, oraz sposób, w jaki zarządza się ryzykiem wynikającym z działań wnioskodawcy i innych podmiotów; [4.5.1.1 lit. a)]*
- *wnioskodawca przedstawia dowody potwierdzające, że sporządził (lub dokonał ustaleń w celu sporządzenia) roczne sprawozdanie dotyczące bezpieczeństwa obejmujące kwestie wymienione w pkt 4.5.1.2 powyżej; [4.5.1.2 lit. a)–f)]*

- *wnioskodawca powinien wskazać, w jaki sposób działa system zarządzania dokumentami, w tym w jaki sposób udostępnia się informacje i są one odpowiednie do wykorzystania w miejscu i czasie, w którym są potrzebne; jak są zmieniane w sposób kontrolowany w ramach systemu i jak są przechowywane i utrzymywane w sposób zapewniający ich łatwe odzyskanie. System zarządzania dokumentami powinien umożliwiać przechowywanie informacji w miejscach, które zapewniają odpowiednie warunki do minimalizacji zniszczeń lub uszkodzeń oraz zapobiegania ich utracie. (4.5.2.1), (4.5.3.1)*

#### 4.5.5 Przykłady dowodów

Opis systemu zarządzania bezpieczeństwem, jego ogólnej struktury i powiązań z dokumentami, które wspierają opisane w nich procesy (np. podręcznik, procedury organizacyjne i operacyjne, instrukcje służbowe). Niezależnie od nowej koncepcji dokumentacji wprowadzonej przez ISO, organizacja może zachować tradycyjną strukturę dokumentacji, jeśli jest ona odpowiednia dla danego celu.

Zarys sposobu, w jaki konstruuje się, publikuje, udostępnia, wypełnia, utrzymuje/zmienia i uchyla poszczególne dokumenty, z odniesieniem do odnośnych procedur kontroli dokumentów.

Procedura sporządzania rocznego sprawozdania, wraz z kopią poprzedniej wersji; jeżeli wnioskodawca jest nowy, procedura określa proponowany układ sprawozdania.

Ustala się, dokumentuje i przestrzega okresów przechowywania dokumentów.

Uwzględnienie czynników ludzkich i organizacyjnych oraz poprawa kultury bezpieczeństwa będą miały pozytywny wpływ na spełnienie odpowiedniego wymogu systemu zarządzania bezpieczeństwem, a dowody na to można znaleźć w następujących źródłach:

Proces lub procedura zarządzania dokumentami dotyczy sposobu, w jaki aktualizuje się dokumenty po regularnych przeglądach oraz po wypadkach lub incydentach. Proces ten lub procedura dotyczy procedury eskalacji, w przypadkach gdy nie dokonano uzgodnionych aktualizacji w wymaganym terminie lub przy braku porozumienia w sprawie sposobu aktualizacji dokumentu.

Istnieje język kontrolowany (tzn. używanie krótkich, zrozumiałych zdań i unikanie żargonu), który stosuje się, aby wspierać wzajemne zrozumienie i dane dobrej jakości.

W miarę możliwości określa się charakter zmian w dokumencie lub w odpowiednich załącznikach w celu usprawnienia ich przeglądu i zatwierdzenia oraz zrozumienia przez pracowników.

Proces opracowywania procedur wyjaśnia, w jaki sposób uwzględnia się w nim czynniki ludzkie i organizacyjne, np.:

- *treść i znaczenie: znaczenie dla zadania wykonywanego przez osobę/osoby, w tym sposób, w jaki operatorzy pierwszej linii aktywnie uczestniczą w opracowywaniu tych procedur;*
- *przepływ: sposób definiowania opisu procesów i odpowiednich obowiązków (kto co robi), poparty wykresami;*
- *zakres: integracja szerszego scenariusza działania w celu zapewnienia zrozumienia danych wejściowych i wyjściowych w odniesieniu do realizowanego zadania;*
- *interfejsy: zawiera wyczerpującą identyfikację i opis interfejsów. Jest jasne, kiedy procedura powinna być stosowana, a kiedy nie ma już zastosowania ze względu na zmiany w zadaniu lub sytuacji pracowej. Jasny cel i zasady zakresu stosowania procedury;*
- *ważność: zaktualizowane i dostarczone w odpowiednim czasie do zrealizowania;*
- *adekwatność i kompleksowość: adekwatność co do tego, jak należy wykonać pracę, i kompleksowość wszystkich niezbędnych szczegółów;*



- *świadomość: pracownicy dobrze rozumieją istniejące procedury/zasady/wymogi, pracownicy rozumieją powody w zakresie bezpieczeństwa dotyczące procedur i potencjalny wpływ ich nieprzebrzegania na działania operacyjne;*
- *działanie/reakcja: procedury jasno pokazują, jakie działania są konsekwencją każdego komunikatu i jaka jest oczekiwana reakcja;*
- *działanie w warunkach stresu/kryzysu: procedury są łatwe do wykonania w warunkach stresu w sytuacji kryzysowej;*
- *elastyczność: procesy pozwalają pracownikom na elastyczność w reagowaniu w sytuacjach awaryjnych, aby zminimalizować negatywne konsekwencje;*
- *konsultacje z pracownikami: w trakcie opracowywania procedur prowadzone są konsultacje z pracownikami – oni najlepiej wiedzą, jak wykonać daną pracę – i mogą przedstawić uwagi lub alternatywne rozwiązania;*
- *okres próbny: procedura przechodzi okres próbny, a przed wejściem w życie następuje przegląd wyników;*
- *przegląd: skuteczność procedury podlega okresowemu przeglądowi, a przegląd uwzględnia wyniki monitoringu, audytów i wnioski wyciągnięte z przeszłych wydarzeń. Jest on ukierunkowany na ciągłe doskonalenie i organizacyjne uczenie się;*
- *zarządzanie zmianą: procedury podlegają przeglądowi w przypadku pojawienia się nowych urządzeń lub procesów. Zarządzanie zmianą w ramach procedur jest ważne, ponieważ pozwala na dostosowanie ich do celów i ustaleń przedsiębiorstw oraz zapewnienie zarządzania odpowiednimi rodzajami ryzyka.*

Personel upoważniony do zatwierdzania dokumentów do wydania zapewniający, aby ich treść była właściwa i zrozumiała dla wszystkich użytkowników końcowych (lub odbiorców), do których dokumenty się odnoszą.

#### 4.5.6 Odniesienia i normy

- [Wytyczne dotyczące wymogów w zakresie udokumentowanych informacji ustanowionych w normie ISO 9001:2015, ISO/TC 176/SC2/N1286](#)

#### 4.5.7 Kwestie związane z nadzorem

Kontrola ustaleń umownych zapewnia skuteczny nadzór i kontrolę ryzyka przez organizację (tj. w przypadku zlecenia podwykonawstwa usług).

Ustalenie relacji między stronami kontrolującymi system zarządzania dokumentami i stronami odpowiedzialnymi za aktualizację informacji oraz kontakty z wspomnianymi stronami w praktyce ma krytyczne znaczenie podczas prowadzenia nadzoru. Często właśnie na tym etapie może pojawić się zakłócenie w kontroli dokumentacji, ponieważ dwie części procesu należą do dwóch różnych struktur zarządzania. Mogłoby to doprowadzić np. do sytuacji, w której różne podmioty przypisywałyby różną wagę działaniom związanym z aktualizacją dokumentacji, co mogłoby w rezultacie skutkować opóźnieniami w procesie aktualizowania dokumentacji o informacje dotyczące powiązanych czynników ryzyka.

Możliwość dostępu pracowników do aktualnych informacji/dokumentacji.

Struktura i tryb pracy systemu zarządzania bezpieczeństwem powinny odzwierciedlać rzeczywisty sposób prowadzenia działań, a nie sztucznie nakładać się na zwyczaje i praktykę.

## 4.6 Integracja czynników ludzkich i organizacyjnych

### 4.6.1 Wymóg regulacyjny

- 4.6.1. Organizacja musi wykazać systematyczne podejście w kwestii integracji czynników ludzkich i organizacyjnych w obrębie systemu zarządzania bezpieczeństwem. Podejście to:
- (a) obejmuje opracowanie strategii oraz wykorzystanie wiedzy fachowej i uznanych metod z dziedziny czynników ludzkich i organizacyjnych;
  - (b) odnosi się do ryzyk związanych z konstrukcją i używaniem sprzętu, zadaniami, warunkami pracy i rozwiązaniami organizacyjnymi, przy uwzględnieniu możliwości i ograniczeń człowieka oraz wpływu na działania człowieka.

### 4.6.2 Cel

Wnioskodawca wykazuje, że stosowanie usystematyzowanego podejścia do czynników ludzkich i organizacyjnych w kierowaniu ryzykiem stanowi integralną część systemu zarządzania bezpieczeństwem. Spełnienie tych kryteriów jest istotne dla wykazania, że wnioskodawca posiada kompetencje wystarczające do prowadzenia działalności kolejowej i włączył systemy kontroli ryzyka do swojego systemu zarządzania bezpieczeństwem, aby zarządzać ryzykiem, z jakim się zmagają.

### 4.6.3 Noty wyjaśniające

Zagadnienie czynników ludzkich i organizacyjnych uwzględnia także spojrzenie systemowe, w ramach którego rozpatrywane są interakcje między czynnikami ludzkimi, technologicznymi i organizacyjnymi. Organizacja powinna uwzględniać czynniki ludzkie i organizacyjne, przyjmując podejście oparte na cyklu życia. Oznacza to zidentyfikowanie i uwzględnienie czynników ludzkich i organizacyjnych w obszarze działań związanych z zarządzaniem bezpieczeństwem, które odnoszą się do celów biznesowych, zarządzania, przewozów, działań człowieka, projektowania zadań i miejsc pracy – na wszystkich etapach cyklu życia systemu, np. od wdrożenia do likwidacji. Strategia dotycząca czynników ludzkich i organizacyjnych określa podejście systemowe do integracji czynników ludzkich i organizacyjnych w obszarze działań związanych z zarządzaniem bezpieczeństwem.

Organizacja powinna rozwijać niezbędne kompetencje w zakresie czynników ludzkich i organizacyjnych, których potrzebuje, aby wspierać swoją działalność biznesową, szczególnie w zakresie ról związanych z bezpieczeństwem. Dotyczy to również pracowników odpowiedzialnych za włączanie czynników ludzkich i organizacyjnych do oceny ryzyka. Specjalistyczna wiedza na temat czynników ludzkich i organizacyjnych oznacza, że zaangażowany personel odbył specjalne szkolenie określone w systemie zarządzania kompetencjami. Posiadanie specjalistycznej wiedzy na temat czynników ludzkich i organizacyjnych oznacza albo posiadanie personelu przeszkolonego na odpowiednim poziomie w celu spełnienia wymogu, albo dostęp do osoby wykwalifikowanej w tym zakresie zgodnie z określonym standardem krajowym lub międzynarodowym. Duże organizacje mogą posiadać dział zajmujący się czynnikami ludzkimi oraz ekspertów w dziedzinie czynników ludzkich, którzy służą organizacji pomocą. Niewielka organizacja może przydzielić odpowiedzialności osobom zarządzającym na wszystkich szczeblach do identyfikowania zewnętrznego zapotrzebowania na wiedzę fachową z zakresu czynników ludzkich.

Wymóg ten związany jest z czynnikami ludzkimi i organizacyjnymi. Więcej informacji na temat strategii dotyczącej czynników ludzkich i organizacyjnych można znaleźć w części Załącznik 5.

#### 4.6.4 Dowody

- *Wnioskodawca uwzględnia w strategii szczegóły dotyczące sposobu, w jaki kwestie związane z czynnikami ludzkimi i organizacyjnymi są systematycznie integrowane, tak aby ryzyko związane z interakcjami pomiędzy zachowaniem człowieka, warunkami organizacyjnymi oraz technologią zostało odpowiednio uwzględnione w ramach procesów systemu zarządzania bezpieczeństwem. Poza tym wnioskodawca powinien jasno wskazać, gdzie można znaleźć dalsze informacje szczegółowe dotyczące odpowiednich procedur lub plany działania na rzecz stopniowej integracji/rozwoju, wskazując działania, kto będzie za nie odpowiedzialny oraz ramy czasowe; **(4.6.1)***
- *stosowane są dostępne standardy projektów uwzględniające czynniki ludzkie i organizacyjne oraz najlepsze praktyki. Przykładem takich norm są np. ISO serii 11064 „Ergonomiczne projektowanie centrów sterowania” oraz ISO serii 9241 „Ergonomia interakcji człowieka i systemu”;*
- *skoncentrowany na użytkowniku proces projektowania, oparty na zasadach i metodach uwzględniających czynniki ludzkie i organizacyjne, a także na zaangażowaniu użytkowników, jest stosowany na przykład w odniesieniu do nowego lub zmodyfikowanego projektu, procedur, szkoleń, obciążenia pracą i środowiska pracy w celu zapewnienia bezpieczeństwa i długotrwałej skuteczności systemu. Użytkownicy końcowi są zaangażowani w proces projektowania, np. w definiowanie wymagań, oraz na późniejszych etapach przy wdrażaniu projektu i jego testowaniu; skoncentrowany na użytkowniku proces projektowania jest procesem iteratywnym, który obejmuje kilka etapów. Analizy prowadzone są w celu określenia specyfiki pracy (np. analiza z zakresu personelu i jego kompetencji, wykonywanych zadań, analiza ryzyka). Na podstawie wyników analiz określone są wymagania w stosunku do użytkowników. Projektowane rozwiązania powinny zawierać określenie interfejsów, stanowisk pracy, szkoleń, procedur oraz organizacji pracy w celu spełnienia wymagań użytkowników. Ocena projektów powinna być dokonana przy użyciu sformalizowanych metod, tj. metody analizy hierarchii zadań, symulacji, ocen ryzyka, ocen ekspertów, ocen użytkowników, weryfikacji i walidacji. W szczególności dotyczy to włączenia czynników ludzkich i organizacyjnych do oceny ryzyka, informacji i komunikacji oraz udokumentowanych informacji; **(3.1, 4.4 i 4.5)***
- *producenci i dostawcy są zaangażowani i świadomi czynników ludzkich przy projektowaniu pojazdów, wyposażenia (interfejs człowiek-maszyna) i systemów informatycznych, a niezbędne wymagania wynikające z procesu opisanego w powyższym punkcie są zawarte w specyfikacjach i umowach; **(5.2)***
- *partnerzy, dostawcy i wykonawcy są zaangażowani w promocję i integrację czynników ludzkich i organizacyjnych; **(5.3)***
- *procedury oceny działania obejmują zasady i metody dotyczące czynników ludzkich i organizacyjnych, przekazywane w sposób kaskadowy z oceny ryzyka; **(6)***
- *procesy doskonalenia, w tym badanie wypadków, obejmują analizę czynników ludzkich i organizacyjnych. **(7)***

#### 4.6.5 Przykłady dowodów

Kopia strategii dotyczącej czynników ludzkich i organizacyjnych, w której opisuje się szczegółowo, w jaki sposób uwzględnia się wykorzystanie wiedzy fachowej oraz technik dotyczących czynników ludzkich i organizacyjnych. Strategia w zakresie bezpieczeństwa odnosi się do strategii dotyczącej czynników ludzkich i organizacyjnych.

Organizacja przeprowadza analizę ryzyka, za pomocą metod empirycznych będących częścią procesów operacyjnych i procesów wspierania, na wszystkich etapach cyklu życia, tj. od projektu aż po zakończenie

użytkowania. W analizie wskazuje się wszystkie czynniki ludzkie i organizacyjne oraz czynniki mające wpływ na funkcjonowanie, które mogą oddziaływać na bezpieczeństwo kolei oraz na działania związane z zarządzaniem bezpieczeństwem, które są potrzebne do kontroli zidentyfikowanych rodzajów ryzyka.

W strategii dotyczącej czynników ludzkich i organizacyjnych przedstawia się wdrożone działania związane z zarządzaniem bezpieczeństwem, a także podejście mające na celu monitorowanie i usprawnianie skuteczności strategii. Strategia opiera się na podejściu proaktywnym, ale, w razie potrzeby, uwzględnia również działania reaktywne.

Metody uwzględniające czynniki ludzkie, np. analiza zadań i analiza użyteczności, są wykorzystywane jako wkład w projektowanie, strukturę i treść procedur, a symulacje w pełnej skali obejmują aktualny personel operacyjny w celu optymalizacji procedur. Działania związane z zarządzaniem bezpieczeństwem, które są powiązane z funkcjami wsparcia, projektowaniem zadań, poziomem zatrudnienia, szkoleniami, projektowaniem i wykorzystywaniem wyposażenia oraz procedurami i protokołami komunikacyjnymi są identyfikowane i powiązane z wynikami oceny ryzyka.

Strategia uwzględnia integrację czynników ludzkich i organizacyjnych w procesie zarządzania zmianą. Integracja czynników ludzkich oznacza proces włączania czynników ludzkich i ergonomii do procesu inżynierii systemów. Plan integracji czynników ludzkich zapewnia usystematyzowane podejście do określenia relacji między wszystkimi działaniami wynikającymi z projektu a czynnikami ludzkimi. Projektowanie czynników ludzkich oznacza włączanie cech ludzkich w definicję, projekt, opracowanie i ocenę systemu, tak aby usprawnić współdziałanie ludzi i maszyn w warunkach operacyjnych.

Procesy operacyjne obejmują złożone modele organizacji pracy, dlatego strategia dotycząca czynników ludzkich i organizacyjnych uwzględnia program zarządzania ryzykiem związanym ze zmęczeniem.

Istnieje wyraźny związek między wynikami oceny ryzyka, strategią dotyczącą czynników ludzkich i organizacyjnych oraz celami w zakresie bezpieczeństwa. Te ostatnie obejmują stopniową integrację czynników ludzkich i organizacyjnych, np.: mapowanie rzeczywistej sytuacji przedsiębiorstwa, identyfikację luk, opracowanie planów integracji lub poprawy czynników ludzkich i organizacyjnych w ich systemach zarządzania bezpieczeństwem, tak aby proces i odpowiednia dokumentacja były kontrolowane w czasie.

Istnieje wyjaśnienie dotyczące tego, w jaki sposób strategia lub jej część jest przekazywana pracownikom poprzez różne procesy, takie jak komunikacja polityki bezpieczeństwa, podnoszenie świadomości lub cele w zakresie bezpieczeństwa.

#### 4.6.6 Odniesienia i normy

- *Wickens, C.D., Lee, J.D., Liu, Y & Gordon Becker, S.E (2004). An Introduction to Human Factors Engineering (Wprowadzenie do projektowania czynników ludzkich). New Jersey: Pearson Education. ISBN-13: 978-0131837362*
- *Serie norm ISO, np.*
- *Seria ISO 6385: 2004 Ergonomic principles in the design of work systems (Zasady ergonomii w dziedzinie projektowania systemów pracy)*
- *Seria ISO 11064 Ergonomic design of control centres (Ergonomiczne projektowanie centrów kontroli)*
- *Seria ISO 9241 Ergonomics of human-system interaction (Ergonomia interakcji między człowiekiem i systemem)*
- *Seria ISO 10075 Ergonomic principles related to mental work-load (Zasady ergonomii dotyczące mentalnego obciążenia w pracy)*
- *CENELEC - EN 50126-1 Zastosowania kolejowe – Specyfikacja i demonstracja niezawodności, dostępności, możliwości utrzymania i bezpieczeństwa (RAMS) – Część 1: Ogólny proces RAMS, rozdział 5.6 (w szczególności § 5.6.4)*

- *EEMUA 191. Alarm systems, a guide to design, management and procurement (Systemy alarmowe, poradnik projektowania, zarządzania i zamawiania)*
- *UIC 651 Layout of drivers' cabs in locomotives, railcars, multiple unit trains and driving trailers (Rozkład kabin maszynistów w lokomotywach, wagonach silnikowych, zespołach trakcyjnych i wagonach sterowniczych)*
- *Rail Safety & Standards Board (2008). Understanding Human Factors, a guide for the railway industry (Zrozumienie czynników ludzkich, poradnik dla przemysłu kolejowego)*

#### 4.6.7 Kwestie związane z nadzorem

Należy się upewnić, że czynniki ludzkie zostały uwzględnione w procesach decyzyjnych w odniesieniu do zarządzania ryzykiem poprzez ocenę ryzyka, zarządzanie zmianą i zarządzaniem zasobami.

Należy się upewnić, że w dokumentach operacyjnych widać zaangażowanie w zarządzanie czynnikiem ludzkim za pomocą rozwiązań ergonomicznych (np. rozwiązań przyjaznych dla użytkownika, prostego języka, obrazków pomagających w zrozumieniu instrukcji, łatwego zarządzania aktualizacjami), aby wesprzeć zarządzanie ryzykiem.

Należy się upewnić, że przedsiębiorstwa kolejowe/zarządcy infrastruktury koncentrują się w analizie wykonywanej przez nich w ramach monitorowania efektywności na czynnikach ludzkich jako głównych lub podstawowych przyczynach wypadków, incydentów lub niebezpiecznych zdarzeń.

Należy sprawdzić, czy istnieją udokumentowane przykłady podjętych środków naprawczych, które zostały opracowane w celu usunięcia czynników wpływających na efektywność działań człowieka i zagrażających bezpieczeństwu.

Usprawnianie funkcjonowania  
systemu kolejowego  
na rzecz społeczeństwa.

## 5 Działalność

### 5.1 Planowanie operacyjne i kontrola operacyjna

#### 5.1.1 Wymóg regulacyjny

- 5.1.1. W trakcie planowania, opracowywania, wdrażania i przeglądu swoich procesów operacyjnych organizacja musi zapewnić, by podczas prowadzenia działalności:
- (a) stosowane były kryteria akceptacji ryzyka i środki bezpieczeństwa (zob. pkt 3.1.1 Ocena ryzyka);
  - (b) realizowany(-e) był(y) plan(y) służący(-e) osiągnięciu celów w zakresie bezpieczeństwa (zob. pkt 3.2 Cele w zakresie bezpieczeństwa i planowanie);
  - (c) gromadzone były informacje na potrzeby pomiaru prawidłowego stosowania i skuteczności ustaleń operacyjnych (zob. pkt 6.1 Monitorowanie).
- 5.1.2. Organizacja musi zapewnić, by jej ustalenia operacyjne były zgodne z dotyczącymi bezpieczeństwa wymogami mających zastosowanie technicznych specyfikacji interoperacyjności i odpowiednich przepisów krajowych oraz wszelkimi innymi stosownymi wymogami (zob. pkt 1 Kontekst organizacji).
- 5.1.3. W celu kontrolowania ryzyk w przypadkach istotnych dla bezpieczeństwa działań operacyjnych (zob. pkt 3.1.1 Ocena ryzyka) uwzględnia się co najmniej:
- (a) planowanie istniejących lub nowych tras pociągów i nowych usług kolejowych, w tym wprowadzanie nowych typów pojazdów, konieczność dzierżawy pojazdów lub wynajęcia personelu od podmiotów zewnętrznych oraz wymianę informacji na temat utrzymania do celów operacyjnych z podmiotami odpowiedzialnymi za utrzymanie;
  - (b) opracowywanie i wdrażanie rozkładów jazdy pociągów;
  - (c) przygotowywanie pociągów lub pojazdów przed przemieszczeniem, obejmujące kontrole przed odjazdem i skład pociągu;
  - (d) poruszanie się pociągów lub przemieszczanie pojazdów w różnych warunkach prowadzenia działalności (w warunkach normalnych, w sytuacji awarii oraz w sytuacji kryzysowej);
  - (e) dostosowanie działalności do wniosków o wycofanie z eksploatacji oraz powiadomień o przywróceniu do eksploatacji wydanych przez podmioty odpowiedzialne za utrzymanie;
  - (f) zezwolenia na przemieszczanie pojazdów;
  - (g) możliwość użytkowania interfejsów w kabinach maszynisty i centrach sterowania pociągiem oraz z wyposażeniem wykorzystywanym przez pracowników odpowiedzialnych za utrzymanie.
- 5.1.3 W celu kontrolowania ryzyk w przypadkach istotnych dla bezpieczeństwa działań operacyjnych (zob. pkt 3.1.1 Ocena ryzyka) uwzględnia się co najmniej:
- (a) określenie granic bezpiecznego transportu na potrzeby planowania ruchu i sterowania ruchem w oparciu o cechy konstrukcyjne infrastruktury;

- (b) planowanie ruchu, w tym rozkład jazdy i alokację tras pociągów;
- (c) zarządzanie ruchem w czasie rzeczywistym w trybie normalnym i w trybach awaryjnych przy zastosowaniu ograniczeń użytkownika oraz zarządzanie zakłóceniami w ruchu;
- (d) określanie warunków dla transportu ładunków nadzwyczajnych.

5.1.4. W celu kontroli podziału odpowiedzialności w przypadkach istotnych dla bezpieczeństwa działań operacyjnych organizacja musi określić odpowiedzialność za planowanie i eksploatację sieci kolejowej, jak również określić sposób podziału odpowiedzialnych zadań mających wpływ na bezpieczne świadczenie wszystkich usług między kompetentnych pracowników w obrębie organizacji (zob. pkt 2.3 Funkcje, odpowiedzialność, rozliczalność i uprawnienia w ramach organizacji) oraz inne zewnętrzne kwalifikujące się podmioty w stosownych przypadkach (zob. pkt 5.3 Wykonawcy, partnerzy i dostawcy).

5.1.4 W celu kontroli podziału odpowiedzialności w przypadkach istotnych dla bezpieczeństwa działań operacyjnych organizacja musi określić odpowiedzialność za planowanie i eksploatację sieci kolejowej, jak również określić sposób podziału odpowiedzialnych zadań mających wpływ na bezpieczne świadczenie wszystkich usług między kompetentnych pracowników w obrębie organizacji (zob. pkt 2.3 Funkcje, odpowiedzialność, rozliczalność i uprawnienia w ramach organizacji) oraz inne zewnętrzne kwalifikujące się podmioty w stosownych przypadkach (zob. pkt 5.3 Wykonawcy, partnerzy i dostawcy).

5.1.5. W celu kontroli informowania i komunikowania w przypadkach istotnych dla bezpieczeństwa działań operacyjnych (zob. pkt 4.4 Informowanie i komunikowanie) odpowiedni pracownicy (np. wchodzący w skład drużyn pociągowych) muszą zostać poinformowani o szczegółach wszelkich określonych warunków podróży, w tym o istotnych zmianach, które mogą prowadzić do zagrożeń, czasowych lub stałych ograniczeniach operacyjnych (np. w związku z określonym typem pojazdów lub z określonymi trasami), oraz o warunkach dotyczących nadzwyczajnych ładunków, w stosownych przypadkach.

5.1.5 W celu kontroli informowania i komunikowania w przypadkach istotnych dla bezpieczeństwa działań operacyjnych (zob. pkt 4.4 Informowanie i komunikowanie) odpowiedni pracownicy (np. dyżurni ruchu) muszą zostać poinformowani o szczególnych wymogach dotyczących tras pociągów oraz przemieszczania pojazdów, w tym o istotnych zmianach, które mogą prowadzić do zagrożeń, czasowych lub stałych ograniczeniach operacyjnych (np. w związku z utrzymaniem torów), oraz o warunkach dotyczących nadzwyczajnych ładunków, w stosownych przypadkach.

5.1.6. W celu kontrolowania kompetencji w przypadkach istotnych dla bezpieczeństwa działań operacyjnych (zob. pkt 4.2 Kompetencje) organizacja musi zapewnić, zgodnie z mającymi zastosowanie przepisami (zob. pkt 1. Kontekst organizacji), w odniesieniu do swoich pracowników:

- (a) zgodność z obowiązującymi ich instrukcjami dotyczącymi szkolenia i pracy oraz podjęcie działań naprawczych w sytuacji, gdy są one wymagane;
- (b) specjalistyczne szkolenia w przypadku planowanych zmian mających wpływ na prowadzenie działalności lub na przypisane im zadania;
- (c) przyjęcie odpowiednich środków w następstwie wypadków i incydentów.

### 5.1.2 Cel

Wnioskodawca powinien wykazać, że wdrożył stosowne procesy mające na celu zarządzanie ryzykiem operacyjnym poprzez system zarządzania bezpieczeństwem, w tym procesy mające na celu uzyskanie pewności, że pracownicy rozumieją swoje role, stojące przed nimi ryzyko operacyjne, że posiadają wiedzę na

temat środków kontroli, oraz że posiadają właściwe kompetencje i zostali odpowiednio przeszkoleni, aby tymi środkami zarządzać, zgodnie z dokumentacją systemu zarządzania bezpieczeństwem.

Wnioskodawca powinien zapewnić, aby pojazdy lub infrastruktura były eksploatowane w bezpieczny sposób, zgodnie z odpowiednimi wymogami w różnych warunkach prowadzenia działalności (tj. w warunkach normalnych, w sytuacji awarii oraz w sytuacji kryzysowej), co uwzględnia również wykorzystywanie zasobów do przeprowadzania testów (np. badanie właściwości biegowych przed przyznaniem autoryzacji) oraz w wyjątkowych okolicznościach (np. ładunki nadzwyczajne, takie jak transport wielkich niepodzielnych części, które nie mogą być transportowane w żaden inny sposób, takie jak belki/dźwigary betonowe przeznaczone do budowy mostów itp.).

### 5.1.3 Noty wyjaśniające

W punktach 5.1.3, 5.1.4 i 5.1.5 tekstu prawnego powyżej, w którym wymóg dotyczy zarządzających infrastrukturą, pkt w kolorze czarnym zastępuje się pkt w kolorze **niebieskim**.

Zgodnie z [dyrektywą \(UE\) 2016/798](#) przedsiębiorstwa kolejowe i zarządcy infrastruktury mają obowiązek ustanowienia systemu zarządzania bezpieczeństwem w celu zarządzania zagrożeniami dla bezpieczeństwa związanymi z działalnością kolejową prowadzoną przez te podmioty. Ogólny konsensus w kwestii zarządzania bezpieczeństwem jest taki, że należy zintegrować bezpieczeństwo w ramach zwykłych procesów gospodarczych w możliwie jak największym stopniu. Powodem tego jest fakt, że w takim przypadku działalność skupia się na bezpieczeństwie w takim samym stopniu jak na każdym innym procesie biznesowym, co zmniejsza konflikty między różnymi procesami.

Międzynarodowa Organizacja Normalizacyjna stwierdza w swoich wytycznych (N360) uzupełniających załącznik SL, że celem punktu 8 (Działalność) jest określenie elementów, które należy wdrożyć w ramach działalności organizacji, aby zagwarantować spełnienie wymogów dotyczących systemu zarządzania, jak również zapewnić odniesienie się do najważniejszych zagrożeń i możliwości. Ponadto stwierdza się, że można określić dodatkowe wymogi (dla danej dziedziny) dotyczące planowania operacyjnego i kontroli operacyjnej. W szczególności stwierdza się, że wymogi te nie są szkodliwe dla działalności gospodarczej przedsiębiorstwa, ale zapewniają wystarczające ramy do kontroli sposobu, w jaki zarządza się kluczowymi kwestiami bezpieczeństwa w ramach procesów gospodarczych organizacji.

Dodano bezpośrednie powiązania między wymogami operacyjnymi i innymi wymogami dotyczącymi systemu zarządzania (podobne do podejścia przyjętego w załączniku II do [rozporządzenia \(UE\) 2019/779](#)), aby wyraźnie wskazać, że wymogi operacyjne należy rozpatrywać w odniesieniu do odpowiednich wymogów dotyczących systemu zarządzania (np. planowanie tras dla przedsiębiorstwa kolejowego to działanie, które powinno podlegać ocenie ryzyka). Podejście to nie zostało stworzone z założeniem, że będzie wyczerpujące, ale ma na celu identyfikowanie poszczególnych kwestii, które organy uznają za znaczące (w oparciu o swoje doświadczenia) i które w związku z tym należy zbadać podczas przeprowadzania przez nie oceny lub podejmowania działań nadzorczych. Przedsiębiorstwa kolejowe i zarządcy infrastruktury powinni skupić się nie tylko na tych szczególnych wymogach podczas opracowywania i wdrażania swoich ustaleń związanych z systemem zarządzania bezpieczeństwem (pomijając, na przykład, inne zagrożenia dla bezpieczeństwa). W każdym przypadku przedsiębiorstwa kolejowe i zarządcy infrastruktury muszą zastosować wymogi dotyczące systemu zarządzania bezpieczeństwem (np. ocenę ryzyka, monitorowanie, kompetencje, informowanie i komunikowanie) do wszystkich swoich odnośnych procesów gospodarczych, aby wykazać, że ryzyko dotyczące bezpieczeństwa jest należycie kontrolowane.

Włączenie systemu zarządzania bezpieczeństwem w procesy gospodarcze/operacyjne ma zasadnicze znaczenie, a w celu zrealizowania tego zamiaru organizacja musi dostosować się do mających zastosowanie TSI (**5.1.2**), takich jak TSI OPE oraz do zgłoszonych przepisów krajowych, w przypadku gdy wymogi dotyczące interfejsu nie są w pełni uregulowane w TSI. Państwa członkowskie lub ich organy mogą również opublikować



akceptowalne sposoby spełniania wymagań, aby ułatwić przestrzeganie swoich przepisów krajowych. W stosownych przypadkach należy wziąć pod uwagę przynajmniej następujące procesy operacyjne:

- *obsługa infrastruktury (kontrolowanie tras i sprzętu infrastruktury, autoryzowanie przemieszczeń pojazdów we wszystkich warunkach i zapewnienie utrzymania infrastruktury: torów i systemów sygnalizacji i sterowania ruchem);*
- *obsługa pociągu (opracowywanie tras i odnośnych rozkładów jazdy, zarządzanie przygotowaniem pociągu, zapewnienie kierowania pociągami, asystowanie, badanie, utrzymanie i naprawianie pojazdów);*
- *manewrowanie (przemieszczanie pojazdów w celu zmontowania lub zdemontowania pociągu).*

TSI-OPE są tutaj kluczowe, ponieważ określają „podstawowe zasady funkcjonowania” (FOP), co należy uwzględnić w odnośnych częściach systemu zarządzania bezpieczeństwem, w związku z czym można wykorzystać zgodność z TSI-OPE w celu wykazania zgodności z odnośnymi powyższymi wymogami dotyczącymi systemu zarządzania bezpieczeństwem.

Zarządca infrastruktury powinien określić i zapewnić warunki oraz środki do użytkowania pojazdów do celów testów na sieci w wyznaczonym terminie określonym w art. 21 ust. 3 i 5 dyrektywy (UE) 2016/797 **(5.1.2)**.

Zapisy kontroli zgodności tras obejmują charakterystykę pojazdu/pociągu rozpatrywaną w odniesieniu do planowanych tras eksploatacji, w tym możliwych tras odchyień określonych przez zarządców infrastruktury (zob. TSI OPE, pkt 4.2.2.5).

Charakterystyka tras eksploatacji odbywa się na podstawie rejestru infrastruktury (RINF) lub informacji dostarczonych przez zarządcę infrastruktury.

Jeżeli któraś ze stron stwierdzi problemy, przedsiębiorstwo kolejowe i zarządca infrastruktury powinni wprowadzić wspólne rozwiązanie.

Nowa usługa kolejowa **[5.1.3 lit. a)]** może obejmować nowe rodzaje towarów przeznaczonych do transportu.

„Bezpieczne granice” **[5.1.3 lit. a)]** dla zarządców infrastruktury oznaczają zarówno bezpieczne fizyczne granice infrastruktury, gdy jest to konieczne, jak i granice bezpieczeństwa dla infrastruktury oraz dowodzenia i kontroli, gdy są one wymagane przez ograniczenia projektowe tej infrastruktury.

Przemieszczenie pojazdów **[5.1.3 lit. d)]** ma szersze znaczenie niż przemieszczenie pociągów (tj. planowane przemieszczenie pojazdów) i autoryzacje wydane przed odjazdem pociągu. Może to obejmować również naprawę zepsutego pociągu, przemieszczenie maszyn służących do utrzymania toru lub nieplanowane zastąpienie uszkodzonego pojazdu wchodzącego w skład pociągu przed odjazdem pociągu.

Zgodnie z art. 1.1 karty UIC 502-1 podano następującą definicję terminu „ładunki nadzwyczajne” **(5.1.5)**: „Ładunek uznaje się za nadzwyczajny, jeśli jego zewnętrzne wymiary, waga lub cechy w odniesieniu do wyposażenia stałego lub wagonu przedsiębiorstwa kolejowego zaangażowanego w transport powodują szczególne trudności, w związku z czym ładunek można przyjąć jedynie na specjalnych warunkach technicznych lub specjalnych warunkach prowadzenia działalności.” W TSI OPE transport nadzwyczajny definiuje się jako: „Pojazd lub przewożony ładunek, który ze względu na konstrukcję/projekt, wymiary lub masę nie spełnia parametrów trasy i wymaga specjalnego zezwolenia na ruch oraz może wymagać specjalnych warunków na części lub całej swojej trasie.”

### **Jak uwzględnić czynniki ludzkie i organizacyjne oraz kulturę bezpieczeństwa?**

Wymiana informacji z podmiotami odpowiedzialnymi za utrzymanie i dysponentami do celów operacyjnych na temat utrzymania pojazdu **[5.1.3 lit. a)]** określono w art. 5 ust. 3 [rozporządzenia \(UE\) 2019/779](#). Wymiana informacji obejmuje harmonogram utrzymania i wszelkie ograniczenia wydane przez podmiot odpowiedzialny za utrzymanie podczas utrzymania (planowanie krótkoterminowe).

Odniesienie do opracowania i wdrażania rozkładów jazdy pociągów **[5.1.3 lit. b)]** oznacza, że wnioskodawca powinien wykazać, w jaki sposób, poprzez ocenę ryzyka, zarządza ryzykiem spowodowanym przez działalność w ramach organizacji i na płaszczyźnie oddziaływań pomiędzy podmiotami. Na przykład wnioskodawca musi wykazać, że wziął pod uwagę:

- *• dodatkowe obciążenie pracą personelu zajmującego się sygnalizacją w przypadku zwiększania liczby pociągów kursujących w danych godzinach;*
- *• odpowiednie uzgodnienia operacyjne z odnośnymi zarządcami infrastruktury w związku z zatrzymaniem ruchu, powrotem do normalnego funkcjonowania, wymianą informacji i wszystkimi pozostałymi usługami uznanymi za konieczne;*
- *• zarządzanie ryzykiem związanym z utrzymaniem torów, w przypadkach gdy pociągi kursują 24 godziny na dobę.*

Organizacja stosuje proaktywny proces oceny ryzyka, który umożliwia identyfikację ryzyka mającego zastosowanie do jej działalności kolejowej, w tym ryzyka związanego z interfejsami współdzielonymi oraz ryzyka wynikającego z czynników ludzkich i organizacyjnych (zob. również 3.1). Zmniejsza również ryzyko nadmiernego polegania na odziedziczonych procedurach lub zasadach.

Organizacja stosuje kryteria akceptacji ryzyka, aby określić, czy istniejące działania są wystarczające do utrzymania lub zmniejszenia ryzyka do akceptowalnego poziomu, czy też w przeciwnym razie należy określić nowe działania. Następnie organizacja włącza swoje działania operacyjne i zgodność z TSI w zakresie, w jakim dotyczą one operacji, do swojego procesu monitorowania (zob. sekcja **6 Ocena wyników** poniżej).

Czynniki ludzkie i organizacyjne należy uwzględnić w planowaniu operacyjnym w celu ciągłego doskonalenia kultury bezpieczeństwa w związku z, np. harmonogramem czasu pracy, zarządzaniem zmęczeniem, stresem, środowiskiem pracy (fizycznym i psychospołecznym), miejscami pracy i procesami pracy itp. Ma to na celu zapewnienie, aby konsekwencje zmian lub ustaleń nie miały negatywnego wpływu na działania człowieka i bezpieczeństwo organizacyjne.

#### 5.1.4 Dowody

- *Informacje mające wskazać, że podczas planowania, opracowywania, wdrażania i dokonywania przeglądu swoich procesów operacyjnych wnioskodawca planuje osiągnąć cele w zakresie bezpieczeństwa, stosuje środki związane z oceną ryzyka i monitoruje wyniki, w tym odpowiednie odesłania do miejsc, w których można znaleźć dodatkowe informacje na temat procedur; **[5.1.1 lit. a)–c)]***
- *dowody poświadczające, że organizacja jest świadoma i faktycznie wdraża wszystkie kategorie obowiązkowych wymogów dotyczących bezpieczeństwa, które odnoszą się do jej działalności oraz przedstawiające sposób, w jaki system zarządzania bezpieczeństwem zapewnia zgodność z tymi wymogami;*
- *informacje na temat tego, że wnioskodawca upewnia się, iż jego ustalenia operacyjne są zgodne z mającymi zastosowanie wymogami (przepisami, normami itd.); **(5.1.2)***
- *w ramach zezwolenia na dopuszczenie typu pojazdu do eksploatacji lub zezwolenia na wprowadzenie pojazdu do obrotu zarządca infrastruktury jest w stanie określić i zapewnić **(5.1.2)**:*
  - *zastosowanie warunków operacyjnych w przypadku użytkowania pojazdów do celów testów na sieci w oparciu o informacje przedstawione przez wnioskodawcę w celu wydania zezwolenia;*
  - *wszelkie niezbędne środki, które mają zostać zastosowane po stronie infrastruktury w celu zapewnienia bezpiecznego i rzetelnego prowadzenia działalności podczas przeprowadzania testów w obrębie sieci, lub*
  - *wszelkie niezbędne środki, które należy zastosować w urządzeniach infrastruktury w celu przeprowadzenia testów w obrębie sieci;*

- w celu kontroli przed rozpoczęciem użytkowania pojazdów, które uzyskały zezwolenie (art. 23 ust. 1 [dyrektywy \(UE\) 2016/797](#)), a zwłaszcza kontroli kompatybilności z trasą (art. 23 ust. 1 lit. a) [dyrektywy \(UE\) 2016/797](#)), przedsiębiorstwo kolejowe, w ramach swojego systemu zarządzania bezpieczeństwem, jest w stanie zidentyfikować i dostarczyć **[5.1.3 lit. a)]** procedury dowodowe i zapisy wykazujące, że pojazd jest kompatybilny z trasą, na której ma być eksploatowany i jest odpowiednio zintegrowany w zestawieniu pociągu (zob. również pkt 4.2.2.5 TSI OPE);
- dowody potwierdzające zgodność dokumentacji operacyjnej z wymogami dotyczącymi zarządzaniem działalnością (i utrzymaniem) blisko granic organizacyjnych i fizycznych, np. powiązania organizacyjne, techniczne i operacyjne z sąsiadującą infrastrukturą, stacje będące przejściem granicznym, interakcje z innymi przedsiębiorstwami kolejowymi i zarządcami infrastruktury itp.; **(5.1.2)**
- informacje dotyczące sposobu, w jaki zarządza się działaniami operacyjnymi za pomocą procesu oceny ryzyka, oraz jak te działania obejmują kwestie przedstawione w wymogach powyżej, w tym czynniki ludzkie i organizacyjne; **[5.1.3 lit. a)–g)]**
- dowody potwierdzające, że organ odpowiedzialny za utrzymanie przestrzega art. 14 ust. 2 [dyrektywy \(UE\) 2016/798](#); **[5.1.3 lit. f)]**
- informacje dotyczące sposobu, w jaki zarządza się obowiązkami, w tym obowiązkami dotyczącymi zarządzania ryzykiem związanym ze zmęczeniem, w odniesieniu do bezpieczeństwa działań operacyjnych; **(5.1.4)**
- informacje dotyczące sposobu, w jaki organizacja zarządza informacją i komunikacją w odniesieniu do bezpieczeństwa działań operacyjnych; **(5.1.5)**
- informacje na temat systemu zarządzania kompetencjami i związanych z nim procedur oraz w jaki sposób te elementy są powiązane z konkretnymi instrukcjami służbowymi lub instrukcjami dotyczącymi zadań, które mają na celu utrzymanie bezpieczeństwa działań operacyjnych; **(5.1.6)**
- dowody potwierdzające, że dokumentacja operacyjna (procedury, instrukcje służbowe, itp.) jest w stosownych przypadkach aktualizowana. **(zob. również 4.5.3)**

#### 5.1.5 Przykłady dowodów

Wykaz obowiązujących wymogów (w tym TSI) oraz opis, w jaki sposób organizacja ich przestrzega (**zob. również 2**).

Wyjaśnienie tego, w jaki sposób zarządza się ryzykiem operacyjnym poprzez proces oceny ryzyka i w jaki sposób zapewnia się, aby cele w zakresie bezpieczeństwa były realizowane. Zapewnia się odniesienia pozwalające znaleźć stosowne procedury.

Deklaracja dotycząca sposobu, w jaki system zarządzania kompetencjami przyczynia się do kontroli ryzyka operacyjnego, i sposobu, w jaki zarządza się przepływem informacji w celu zapewnienia, aby ryzyko było właściwie kontrolowane.

Informacje szczegółowe dotyczące systemu utrzymania taboru organizacji.

Szczegółowe procedury dotyczące kontroli przed odjazdem (TSI OPE), które zostały wprowadzone w celu zapewnienia sprawdzenia zgodności z wymogami:

- efektywności hamowania (przygotowanie tabeli hamowania);
- składu pociągu;
- przednich i tylnych sygnałów;
- obciążenia i stanu ciągnionego pojazdu.

Kopia opisu procesu dotyczącego identyfikowania przypadków braku zgodności z wymogami oraz informacje dotyczące sposobu, w jaki zapewnia się podejmowanie wszelkich koniecznych działań, w tym takich, które

prowadzą do wyłączenia pojazdu z działalności, wymiany zepsutego/wadliwego komponentu/wyposażenia/pojazdu lub zastosowania ograniczeń operacyjnych.

Dokument, w którym przedstawiono rodzaje pojazdów, które mają być wykorzystywane na każdej określonej trasie, oraz rodzaj działalności, która ma być prowadzona, a w szczególności wszelkie:

- *ograniczenia operacyjne związane z określonymi rodzajami pojazdów;*
- *ograniczenia związane z eksploatacją określonych rodzajów pojazdów na określonych trasach;*
- *dotatkowe wymogi związane z utrzymaniem dotyczące określonych tras (zob. również 5.2).*

W odniesieniu do kwestii zgodności z podstawowymi zasadami operacyjnymi (FOP) zawartymi w TSI OPE przedstawia się dowody potwierdzające, że przedsiębiorstwo kolejowe jest w stanie zapewnić, aby (tylko w celu zobrazowania):

- *Pociąg mógł być eksploatowany na danej części trasy tylko, jeśli skład pociągu jest zgodny z daną infrastrukturą (FOP 3)*

*Dotyczy to upewnienia się, że pociąg jest zgodny z infrastrukturą trasy, na której ma być eksploatowany, zanim zostanie dopuszczony do ruchu. Zgodność pociągu z infrastrukturą zależy głównie od wymiarów pojazdu i ładunku na nim umieszczonego; przeswitów między pociągiem i infrastrukturą lub pociągami znajdującymi się na sąsiednich torach (przeprowadzanie pomiarów); minimalnej zdolności pociągu do hamowania; wagi i długości pociągu oraz przepustowości i wydajności infrastruktury.*

Istnieją dowody na to, że:

- *są przeprowadzane kontrole przed odjazdem w celu zapewnienia bezpiecznego przewozu pasażerów, personelu i towarów, zanim pociąg rozpocznie podróż lub będzie ją kontynuował (FOP 4)*

*Dotyczy to pociągu i jego gotowości do wyruszenia. Uwzględnia to na przykład: zdolność pociągu do hamowania, dozwoloną prędkość poruszania się pociągu, skład i sprzęgi pociągu, identyfikację, załadunek i zabezpieczenie ładunku, udzielenie wystarczających informacji pracownikom zajmującym się przygotowaniem pociągu i jego eksploatacją. Ma to na celu zapobiegnięcie kolizjom i wykolejeniom spowodowanym różnymi zagrożeniami.*

Uwzględnienie czynników ludzkich i organizacyjnych oraz poprawa kultury bezpieczeństwa będą miały pozytywny wpływ na spełnienie odpowiedniego wymogu systemu zarządzania bezpieczeństwem, a dowody na to można znaleźć w następujących źródłach:

W dokumencie, w którym opisano wszelkie dodatkowe wymogi dotyczące zarządzania sytuacjami awaryjnymi (np. incydentami z udziałem pojazdu) w odniesieniu do sieci właściwej dla obszaru działalności.

Osoby odpowiedzialne za planowanie i realizację działań operacyjnych są przeszkolone w zakresie uwzględniania czynników ludzkich i organizacyjnych, zarówno w celu zintegrowania możliwości i ograniczeń wykonawczych człowieka, jak i w celu uwzględnienia zidentyfikowanych ryzyk i środków bezpieczeństwa.

Określenie informacji dotyczących bezpieczeństwa i przestrzeganie zasad dotyczących czynników ludzkich i organizacyjnych (zob. sekcja **4.4 Informowanie i komunikowanie** poniżej).

W procesie dotyczącym zarządzania zmęczeniem, który ma zastosowanie do pracowników o nieregularnym czasie pracy. Proces jest oparty na metodach empirycznych i wiedzy fachowej. W procesie bierze się pod uwagę konieczność rozpatrzenia szerokiego zakresu czynników przy stosowaniu kompleksowego podejścia mającego na celu zarządzanie ryzykiem związanym ze zmęczeniem. Program zarządzania zmęczeniem uwzględnia planowanie i kontrolę środowiska pracy i zadań służbowych w celu minimalizacji, w miarę możliwości, wpływu zmęczenia na czujność i funkcjonowanie załogi w sposób, który jest odpowiedni dla poziomu ryzyka, na jakie pracownicy są narażeni, oraz charakteru działalności.

### 5.1.6 Odniesienia i normy

- *ISO N360 JTCG dokument koncepcyjny uzasadniający załącznik SL*
- [Broszura UIC 502-1](#)
- [Załącznik II do dyrektywy 2008/68/WE \(RID\)](#)
- [Wytyczne dotyczące TSI OPE](#)

### 5.1.7 Kwestie związane z nadzorem

Nadzór nad działaniami operacyjnymi powinien być prowadzony poprzez skupienie się na konkretnych sprawach oraz ich szczegółową analizę w celu sprawdzenia, w jaki sposób znajdują odzwierciedlenie w systemie zarządzania bezpieczeństwem organizacji, która jest poddawana nadzorowi, i czy organizacja rozmieściła właściwych pracowników we właściwych miejscach, którzy wykonują właściwe czynności. Umożliwi to krajowemu organowi ds. bezpieczeństwa sprawdzenie, czy działania są objęte systemem zarządzania bezpieczeństwem jako spójna całość, czy są zarządzane oddzielnie, w sposób słabo powiązany z celami w zakresie bezpieczeństwa i ogólną strategią.

W ramach działań nadzorczych należy szczególnie sprawdzić:

- *W jaki sposób dokumenty SMS, które służą do zarządzania ryzykiem na poziomie operacyjnym, przekładają się na instrukcje robocze na stanowiskach pracy;*
- *zarządzanie w okolicznościach kryzysowych lub sytuacjach wybiegających poza normę;*
- *sposób zarządzania granicami/ograniczeniami działalności, w tym ustalenia z innymi stronami dotyczące współdziałania;*
- *ustalenia dotyczące zarządzania zmęczeniem;*
- *zarządzanie substancjami niebezpiecznymi;*
- *ustalenia dotyczące transportu towarów niebezpiecznych, w tym szkolenia, role oraz obowiązki przydzielone pracownikom organizacji, jak określono w rozdziałach 1.3 i 1.4 oraz 1.8. regulaminu RID, współpracując w razie potrzeby z jakimkolwiek innym właściwym organem do spraw transportu towarów niebezpiecznych;*
- *zgodność z podstawowymi zasadami funkcjonowania opisanymi w TSI OPE.*

## 5.2 Zarządzanie składnikami aktywów

### 5.2.1 Wymóg regulacyjny

|   |
|---|
| <p>5.2.1. Organizacja musi zarządzać ryzykami dla bezpieczeństwa związanymi z rzeczowymi składnikami aktywów przez cały cykl życia tych aktywów (zob. pkt 3.1.1 Ocena ryzyka), tj. od projektu aż po zakończenie użytkowania, oraz spełniać wymagania w zakresie czynników ludzkich na wszystkich etapach cyklu życia.</p> <p>5.2.2. Organizacja musi:</p> <ul style="list-style-type: none"><li>(a) zapewnić, by składniki aktywów były wykorzystywane w zamierzonym celu przy jednoczesnym utrzymaniu ich bezpiecznego stanu eksploatacyjnego, w stosownych przypadkach zgodnie z art. 14 ust. 2 dyrektywy (UE) 2016/798, oraz ich oczekiwanego poziomu działania;</li><li>(b) zarządzać składnikami aktywów w normalnych warunkach działalności i w sytuacji awarii;</li><li>(c) wykrywać tak szybko, jak jest to w rozsądny sposób wykonalne, przypadki nieprzestrzegania wymogów eksploatacyjnych przed lub w trakcie eksploatacji składnika aktywów, co obejmuje również stosowanie ograniczeń użytkowania, jeśli jest to właściwe dla zapewnienia bezpiecznego stanu eksploatacyjnego składnika aktywów (zob. pkt 6.1 Monitorowanie).</li></ul> <p>5.2.3. Organizacja musi zapewnić, by jej ustalenia dotyczące zarządzania składnikami aktywów były w stosownych przypadkach zgodne ze wszystkimi zasadniczymi wymaganiami określonymi w odpowiednich technicznych specyfikacjach interoperacyjności oraz wszelkimi innymi stosownymi wymogami (zob. pkt 1. Kontekst organizacji).</p> <p>5.2.4. W celu kontrolowania ryzyk w przypadkach istotnych dla zapewnianych usług utrzymania (zob. pkt 3.1.1 Ocena ryzyka) uwzględnia się co najmniej:</p> <ul style="list-style-type: none"><li>(a) określenie potrzeb w zakresie utrzymania, tak aby utrzymywać składnik aktywów w bezpiecznym stanie eksploatacyjnym, na podstawie planowanego i faktycznego wykorzystania składnika aktywów oraz jego cech konstrukcyjnych;</li><li>(b) zarządzanie wycofaniem składnika aktywów z eksploatacji na potrzeby utrzymania, w przypadku stwierdzenia usterek lub gdy stan składnika aktywów ulega pogorszeniu w stopniu przekraczającym granice bezpiecznego stanu eksploatacyjnego, o którym mowa w lit. a);</li><li>(c) zarządzanie przywróceniem składnika aktywów do eksploatacji, z ewentualnymi ograniczeniami użytkowania po przeprowadzeniu konserwacji mającej na celu zapewnienie jego bezpiecznego stanu eksploatacyjnego;</li><li>(d) zarządzanie sprzętem służącym do monitorowania i pomiarów, tak aby zapewnić, że jest on odpowiedni do zamierzonego celu.</li></ul> <p>5.2.5. W celu kontroli informowania i komunikowania w przypadkach istotnych dla bezpiecznego zarządzania aktywami (zob. pkt 4.4 Informowanie i komunikowanie) organizacja musi uwzględnić:</p> <ul style="list-style-type: none"><li>(a) wymianę odpowiednich informacji w ramach organizacji lub z zewnętrznymi podmiotami odpowiedzialnymi za utrzymanie (zob. pkt 5.3 Wykonawcy, partnerzy i dostawcy), w szczególności informacji dotyczących związanych z bezpieczeństwem nieprawidłowości, wypadków i incydentów oraz dotyczących ewentualnych ograniczeń użytkowania składnika aktywów;</li></ul> |
|---|

- (b) identyfikowalność wszystkich niezbędnych informacji, w tym informacji dotyczących lit. a) (zob. pkt 4.4 Informowanie i komunikowanie oraz pkt 4.5.3 Kontrola dokumentacji);
- (c) ustanowienie i utrzymywanie dokumentacji, w tym zarządzanie zmianami mającymi wpływ na bezpieczeństwo składników aktywów (zob. pkt 5.4 Zarządzanie zmianą).

### 5.2.2 Cel

Wnioskodawca powinien wykazać sposób, w jaki zarządza cyklem życia swoich aktywów od projektu aż po zakończenie użytkowania z wykorzystaniem procedur i ustaleń określonych w systemie zarządzania bezpieczeństwem. Wnioskodawca powinien wykazać, że na każdym etapie cyklu życia zastosował podejście zorientowane na człowieka. Powinien dostarczyć informacje szczegółowe opisujące, gdzie zarządzanie aktywami organizacji łączy się z poszczególnymi elementami jej systemu zarządzania bezpieczeństwem, takimi jak zarządzanie kompetencjami, planowanie operacyjne i monitorowanie. Celem wnioskodawcy powinno być wykazanie, że wdrożył sprawny system zarządzania aktywami, który jest odpowiedni dla zagrożeń wynikających z rodzaju i zakresu jego działalności.

### 5.2.3 Noty wyjaśniające

„Aktywa” **(5.2)** oznaczają każde wyposażenie (stałe lub ruchome), strukturę, oprogramowanie lub dowolny inny komponent, który wymaga utrzymania w długim okresie, zapewnione w celach prowadzenia działalności kolejowej. Aktywa zostaną podzielone na te zarządzane przez przedsiębiorstwo kolejowe (głównie pojazdy, ale obejmujące również inne urządzenia, np. tokarki kołowe, sprzęt ochronny i programy komputerowe przewidziane do bezpiecznego utrzymania aktywów) i te zarządzane przez zarządcę infrastruktury (wszystkie pozycje infrastruktury, takie jak tory, urządzenia bezpiecznej kontroli jazdy/sterowania ruchem kolejowym, urządzenia służące do zmiany jednego toru na inny, urządzenia sieci trakcyjnej, przejazdy kolejowe, inżynieria lądowa, taka jak mosty, wiadukty, tunele, perony, windy, ruchome schody itp. Pełny wykaz przedstawiono w załączniku I do [dyrektywy \(UE\) 2012/34](#)).

Cykl życia aktywu obejmuje następujące etapy:

- a) projekt;
- b) realizację (budowę/produkcję, instalację, przeprowadzenie badań i oddanie do użytku);
- c) eksploatację i utrzymanie;
- d) naprawę, wprowadzanie zmian i modernizację, w tym zarządzanie zmianami;
- e) odnowienie, wycofanie z użytku i usunięcie.

Ważne jest, aby organizacja wykazała, w jaki sposób uzyskuje i utrzymuje (systemowo) wymogi bezpieczeństwa dotyczące aktywów oraz w jaki sposób zostaną one zweryfikowane, zwalidowane i śledzone.

W przypadku zlecenia utrzymania aktywów stronie trzeciej to organizacja jest odpowiedzialna za określenie i monitorowanie, czy usługa jest zgodna z ustalonymi standardami organizacji.

Po wdrożeniu procesu zarządzania ryzykiem i zidentyfikowaniu aktywów o istotnym znaczeniu dla bezpieczeństwa organizacja powinna monitorować ryzyko wiążące się z tymi aktywami.

W przypadku gdy istnieje prawdopodobieństwo odnowienia, wycofania z użytku lub usunięcia aktywów, organizacja ustanawia i dokumentuje procesy dotyczące zarządzania wszelkim ryzykiem związanym z takimi działaniami.

Procesy te dotyczą jedynie tych organizacji, które przeprowadzają takie działania lub prawdopodobnie będą je przeprowadzać.

W przypadku odnowienia aktywów, których okres eksploatacji zbliża się do końca, organizacja zapewnia, aby zastępujące aktywa spełniały ustanowione kryteria dotyczące skuteczności działania w zakresie bezpieczeństwa. Jako część tego procesu wszystkie analizy bezpieczeństwa poddawane są przeglądowi.

Wymogi odnoszące się do utrzymania **(5.2.4)** pochodzą z rozporządzenia w sprawie podmiotów odpowiedzialnych za utrzymanie, tabor kolejowy to aktywa, którymi powinno zarządzać przedsiębiorstwo kolejowe i ewentualnie zarządca infrastruktury. Wymogi określone w załączniku II do [rozporządzenia \(UE\) 2019/779](#) są bardziej szczegółowe i mają charakter nakazowy, podczas gdy powyższe wymogi odnoszą się głównie do elementów wspólnych między przedsiębiorstwem kolejowym lub systemem zarządzania bezpieczeństwem zarządcy infrastruktury i systemem utrzymania podmiotu odpowiedzialnego za utrzymanie w celu zapewnienia, aby eksploatacja i utrzymanie aktywów było bezpieczne. Dodatkowe informacje szczegółowe można znaleźć w rozporządzeniu w sprawie podmiotów odpowiedzialnych za utrzymanie oraz w towarzyszącym mu przewodniku. Ocena ryzyka powinna odnosić się również do potencjalnego wpływu na bezpieczeństwo każdego zastąpienia w ramach utrzymania (co jest częścią cyklu życia aktywu) zgodnie z wymogami [dyrektywy \(UE\) 2016/797](#) i odnośnych TSI.

TSI nie regulują wszystkich aktywów **(5.2.3)**, a nawet jeśli TSI ma zastosowanie (np. TSI INF), uregulowane są jedynie kwestie niezbędne dla interoperacyjności, co oznacza, że nadal mogą być potrzebne inne wymogi dotyczące bezpieczeństwa. Zgodność z kluczowymi wymogami odnośnych TSI (nie tylko kluczowymi wymogami w zakresie bezpieczeństwa) należy utrzymać w przypadku zastąpienia, odnowienia lub modernizacji.

Termin „bezpieczny stan eksploatacyjny” **[5.2.4 lit. a)]** oznacza, że aktywa należy eksploatować w bezpiecznych granicach ich użytkowania. Granice bezpieczeństwa użytkowania mogą się zmienić w trakcie okresu funkcjonowania systemu, ale należy je określić, mając na względzie parametry interoperacyjności. Wady można zidentyfikować **[5.2.4 lit. b)]** i w oparciu o analizę podstawowych przyczyn odpowiednio dostosować granice bezpieczeństwa użytkowania. Zgodnie z art. 14 ust. 2 [dyrektywy \(UE\) 2016/798](#) w przypadku pojazdów bezpieczny stan eksploatacyjny oznacza zdolność do poruszania się w bezpieczny sposób.

Konfiguracja aktywów **[5.2.5 lit. c)]** obejmuje jednoznaczne oznaczenie aktywów, ich lokalizację, wszelkie przeprowadzone prace związane z utrzymaniem itp. (nie tylko zarządzanie konfiguracją zmian). Zarządzanie konfiguracją zmian (technicznych) ma zastosowanie w przypadku zastąpienia.

Zgodnie z art. 14 ust. 1 [dyrektywy \(UE\) 2016/798](#) należy wyznaczyć podmiot odpowiedzialny za utrzymanie, aby zapewnić poruszanie się pojazdu przeznaczonego do utrzymania, za który odpowiada podmiot, w bezpieczny sposób. Nie istnieje konieczność szczegółowego opisywania działań przeprowadzonych przez podmiot odpowiedzialny za utrzymanie, który został certyfikowany zgodnie z [rozporządzeniem \(UE\) 2019/779](#). Konieczne jest natomiast wskazanie, które elementy i aspekty obejmuje certyfikat podmiotu odpowiedzialnego za utrzymanie i w jaki sposób zarządza się elementami wspólnymi z podmiotem odpowiedzialnym za utrzymanie, w szczególności jaki rodzaj informacji wymienia się między wnioskodawcą i podmiotem odpowiedzialnym za utrzymanie i w jaki sposób przebiega ta wymiana. Jeżeli przedsiębiorstwo kolejowe nie zawarło bezpośredniej umowy z podmiotem odpowiedzialnym za utrzymanie, lecz podmiot ten jest stroną trzecią umowy pomiędzy właścicielem (lub posiadaczem) pojazdu a przedsiębiorstwem kolejowym, wymiana informacji może odbywać się za pośrednictwem pośrednika, ale nadal musi być skuteczna i terminowa w obu kierunkach.

W przypadkach partnerstwa między przedsiębiorstwami kolejowymi każde przedsiębiorstwo kolejowe pozostaje w pełni odpowiedzialne za bezpieczne prowadzenie działalności, a zatem za kontrolowanie ryzyka związanego z jego działalnością. Korzystanie przez przedsiębiorstwo kolejowe z certyfikatu bezpieczeństwa przedsiębiorstwa kolejowego będącego jego partnerem nie jest wystarczającym środkiem kontroli ryzyka związanego ze świadczeniem usług utrzymania, jeżeli nie stoją za nim ustalenia umowne zawarte między partnerskimi przedsiębiorstwami kolejowymi. Wspomniane ustalenia umowne muszą być wspólnie opracowane i monitorowane przez każdego partnera, przy czym są również częścią każdego systemu



zarządzania bezpieczeństwem, w związku z czym podlegają one nadzorowi przez odpowiednie krajowe organy ds. bezpieczeństwa. Odpowiednie krajowe organy ds. bezpieczeństwa powinny skoordynować swoje działania w celu rozwiązania wszelkich wspólnych kwestii transgranicznych spowodowanych przez podmioty zamawiające.

### ***Jak uwzględnić czynniki ludzkie i organizacyjne oraz kulturę bezpieczeństwa?***

Czynniki ludzkie są zintegrowane w całym cyklu życia wszystkich systemów i podsystemów, w oparciu o wyniki oceny ryzyka, która obejmowała już czynniki ludzkie i organizacyjne oraz zdefiniowane środki bezpieczeństwa.

Obejmuje to podejście skoncentrowane na użytkowniku w fazie projektowania systemu, które może składać się z podziału funkcji (człowiek/maszyna), wywiadów i analiz zadań (w odniesieniu do każdego podzadania). Specyfikacje aktywów są oparte na potrzebach użytkowników, w tym wynikach i ograniczeniach użytkownika.

Środki bezpieczeństwa określa się z uwzględnieniem środowiska pracy, organizacji i personelu, zespołów i komunikacji, projektu procedur (w tym operacji i utrzymania składnika aktywów) oraz odpowiednich zasobów w odniesieniu do składnika aktywów, zapewniając, że czynniki ludzkie i organizacyjne są brane pod uwagę i odpowiednio uwzględniane. Może to obejmować specyfikacje dotyczące np. układu miejsca pracy, ergonomicznego projektu sprzętu (narzędzi, maszyn, materiałów), użyteczności sprzętu, oczekiwanych reakcji, jakości sprzętu, harmonogramu kontroli/utrzymania oraz tolerancji dla błędów.

#### ***5.2.4 Dowody***

- *Informacje dotyczące systemu zarządzania aktywami w ramach systemu zarządzania bezpieczeństwem organizacji, w tym odniesienia do pozostałych obszarów, takich jak ocena ryzyka, planowanie operacyjne, zarządzanie zmianami itp. (5.2.1), (5.2.2), [5.2.5 lit. a)–b]):*

#### ***Etap projektu***

- *dowody potwierdzające procesy i konsultację w celu określenia wymogów dotyczących aktywów;*
- *dowody potwierdzające istnienie strategii na rzecz zarządzania ryzykiem w odniesieniu do zamawiania i oddania do użytku nowych lub zmienionych aktywów;*
- *dokumentacja wszystkich odnośnych procesów związanych z projektowaniem i dostarczaniem aktywów;*
- *procesy dotyczące zarządzania ryzykiem na etapie projektu;*
- *dowody przedstawiające narzędzia wykorzystane do zapewnienia bezpieczeństwa;*
- *szczegóły dotyczące norm lub inne informacje dotyczące bezpieczeństwa, na które powołano się w odniesieniu do projektu i utrzymania aktywów oraz wszelkie testy przeprowadzone w celu potwierdzenia zgodności z wymogami;*
- *istnienie podręcznika lub podobnego dokumentu, który zawiera procesy dotyczące eksploatacji i utrzymania aktywów oraz zarządzania ryzykiem na etapie eksploatacji i utrzymania;*

#### ***Etap realizacji***

- *dowody dotyczące zarządzania ryzykiem w zakresie bezpieczeństwa, przeprowadzania testów i procesów zatwierdzenia obejmujących budowę/produkcję oraz oddanie aktywów do użytku, oraz ich gotowość do eksploatacji;*

**Etap eksploatacji i utrzymania**

- dowody potwierdzające stałą zgodność z normami i procesami oraz zarządzanie zidentyfikowanym ryzykiem;
- plany i procedury dotyczące utrzymania aktywów;
- dowody potwierdzające działalność organizacji w odniesieniu do identyfikowania i eliminowania ryzyka;
- dowody na istnienie procesów do raportowania i zarządzania wszelkimi kwestiami dotyczącymi bezpieczeństwa i działaniami naprawczymi;
- dowody potwierdzające stosowanie metod prognozowania tendencji w zakresie wyników w odniesieniu do przewidywanego okresu strategicznej eksploatacji poszczególnych składników aktywów w celu monitorowania wyników i planowania odnowień;
- procesy dotyczące identyfikowania błędów i awarii oraz podejmowania działań naprawczych;
- zarządzanie w okolicznościach kryzysowych lub sytuacjach wybiegających poza normę, które mogą wpłynąć na bezpieczeństwo aktywów;
- dowody na uwzględnienie zarządzania aktywami w przypadku zdarzeń wymagających zgłoszenia oraz na zarządzanie wspólnym ryzykiem na płaszczyźnie oddziaływań **(zob. również 3.1)**;

**Odnowienie, wycofanie z użytku i usunięcie**

- dowody prezentujące procesy zarządzania ryzykiem związanym z odnowieniem, wycofaniem z użytku lub usunięciem aktywów, które są odpowiednie do skali i charakteru organizacji;
- dowody na systematyczne podejście mające na celu rozwiązanie kwestii związanych z czynnikami ludzkimi i organizacyjnymi na każdym etapie cyklu życia zarządzania aktywami; **(5.2.1)**
- dowody potwierdzające zgodność dokumentacji operacyjnej z wymogami dotyczącymi zarządzania (eksploatacji) i utrzymania blisko granic organizacyjnych i fizycznych, np. powiązania organizacyjne, techniczne i operacyjne z sąsiadującymi infrastrukturami, stacje będące przejściem granicznym, interakcje z innymi przedsiębiorstwami kolejowymi lub zarządcami infrastruktury; **(5.2.3)**;
- informacje, z których wynika, że wnioskodawca wykazał, iż jego ustalenia związane z utrzymaniem są zgodne ze stosownymi wymogami (prawodawstwo, normy itp.); **(5.2.3)**
- w przypadku pojazdów kopia certyfikatu podmiotu odpowiedzialnego za utrzymanie (może on być w posiadaniu przedsiębiorstwa kolejowego lub podmiotu, na którym przedsiębiorstwo kolejowe polega w zakresie utrzymania pojazdów, lub nawet zlecany na zewnątrz w odniesieniu do funkcji utrzymania) lub (do 16 czerwca 2022 r.) dowody na to, że art. 14 ust. 2, art. 14 ust. 3 i załącznik III do [dyrektywy \(UE\) 2016/798](#) są przestrzegane przez podmiot odpowiedzialny za utrzymanie; **[5.2.4 lit. a)–d)]**

W sytuacji, w której pomiędzy przedsiębiorstwami kolejowymi istnieje porozumienie o partnerstwie i pojazd jest utrzymywany przez partnera:

Dowody potwierdzające, że partnerów obowiązują ustalenia umowne, w tym:

- wymiana informacji opisana w art. 5 [rozporządzenia \(UE\) 2019/779](#);
- w stosownych przypadkach wsparcie techniczne, w szczególności w zakresie dotychczasowego systemu kontrolno-decyzyjnego;
- kontrola zdolności zakontraktowanych warsztatów utrzymaniowych do świadczenia usług utrzymania;
- monitorowanie pojazdów oraz wymiana istotnych informacji uzyskanych w drodze tego monitorowania; **(zob. również 6.1)**
- w przypadku aktywów, wobec których w przepisach unijnych lub krajowych wymaga się certyfikatu zgodności, kopia takiego certyfikatu łącznie z wyjaśnieniem, w jakim stopniu na tym się polega w ramach systemu zarządzania bezpieczeństwem; **[5.2.4 lit. a)–d)]**

- *informacje dotyczące sposobu funkcjonowania części systemu zarządzania bezpieczeństwem dotyczącej zarządzania dokumentami w odniesieniu do zarządzania aktywami, w tym dowody potwierdzające, że dokumentacja dotycząca utrzymania (procedury, instrukcje służbowe itp.) jest w stosownych przypadkach aktualizowana; [5.2.5 lit. a)–c)]*
- *dowody na temat zarządzania konfiguracją aktywów w całym okresie ich cyklu życia, w tym wszystkie procesy zarządzania zmianami wdrożone w celu radzenia sobie z działaniami rekonfiguracyjnymi na poziomie podstawowym. [5.2.5 lit. c)]*

#### 5.2.5 Przykłady dowodów

##### **Etap projektu**

Organizacja dokumentuje wszelkie istotne ze względu na bezpieczeństwo procesy i informacje związane z projektowaniem i przygotowaniem aktywów dzięki wykorzystaniu procesów zarządzania konfiguracją (lub systemu zarządzania konfiguracją). Za ich pomocą określa się działania techniczne i organizacyjne, które ustanawiają i utrzymują kontrolę danych aktywów przez cały okres ich cyklu życia.

Organizacja ustanawia i dokumentuje proces mający na celu zarządzanie ryzykiem związanym z projektowaniem rozwiązania dotyczącego danego aktywów poprzez:

- *określenie wymogów dla wszelkich nowych lub zmienionych aktywów (**zob. również 1**) i przeprowadzenie konsultacji na ich temat z odpowiednimi zainteresowanymi stronami (**zob. również 2.4**);*
- *zarządzanie ryzykiem związanym z wdrażaniem takich zmian (**zob. również 3.1**); oraz*
- *zarządzanie ryzykiem związanym z zamawianiem aktywów i, w stosownych przypadkach, zarządzanie umowami (**zob. również 3.1 i 5.3**).*

Obejmuje to analizę zagrożeń, aby zidentyfikować obszary najbardziej narażone na wystąpienie awarii, i zaktualizowanie rejestru zagrożeń. Osiąga się to poprzez wskazanie systemów o istotnym znaczeniu dla bezpieczeństwa i ustalenie kluczowych celów w zakresie skuteczności za pomocą odpowiednich technik identyfikacji ryzyka, np.:

- *analiza projektu aktywów pod kątem niezawodności, dostępności, możliwości utrzymania i bezpieczeństwa (RAMS) (w której informuje się projektantów o kryteriach dotyczących skuteczności działania w zakresie bezpieczeństwa w celu zapewnienia, aby dane aktywa były odpowiednie do celu); i*
- *analiza przyczyn, skutków i krytyczności błędów (FMECA) lub analiza utrzymania skupionego na niezawodności (reliability centred maintenance – RCM) przeprowadzone w celu zarządzania ryzykiem podczas etapu projektu oraz w ramach działań na rzecz ustanowienia planu utrzymania.*

Zarządza się tymi wymogami w odniesieniu do określonych norm i procesów wykorzystywanych w projektowaniu, utrzymaniu i eksploatacji infrastruktury kolejowej i taboru, wedle wskazań organizacji. Organizacja zapewnia, aby:

- *systemy o istotnym znaczeniu dla bezpieczeństwa zostały zaprojektowane zgodnie ze specyfikacjami funkcjonalnymi;*
- *istniał plan testów dotyczący poświadczania i oddawania do użytku mający na celu potwierdzenie, że dane aktywa są odpowiednie do celu, ich eksploatacja i utrzymanie są bezpieczne; oraz*
- *przygotowano dokumentację dotyczącą eksploatacji i utrzymywania, w której określa się procesy dotyczące aktualizacji przeglądu i utrzymania aktywów (**zob. również 4.5**).*

Organizacja wykazuje, że w swoim podejściu do projektowania i zamawiania korzysta z właściwych procesów inżynierii systemów i systemów zapewnienia bezpieczeństwa (np. EN50126/8/9 w przypadku złożonych systemów). Można to osiągnąć poprzez utworzenie „planu zarządzania inżynierią systemów” (SEMP), w

którym określa się procedurę mającą na celu wskazanie i zarejestrowanie zainteresowanych stron, wymagań systemowych oraz potrzeb związanych z bezpieczeństwem.

### ***Etap realizacji***

W celu zapewnienia pomyślnego i bezpiecznego wdrożenia danych aktywów organizacja ustanawia proces mający na celu zarządzanie ryzykiem związanym z ich budową, przeprowadzaniem testów i oddawaniem do użytku, zgodnie z procesami systemu zarządzania bezpieczeństwem.

Wdraża również proces, który ma na celu zarządzanie:

- *testowaniem, weryfikacją i poświadczaniem wymogów systemowych i wymogów dotyczących bezpieczeństwa dotyczących danych aktywów, co można osiągnąć za pomocą „planu zarządzania przeprowadzaniem testów i oddawaniem do użytku” lub jego odpowiednikiem; oraz*
- *gotowością danych aktywów do eksploatacji, co można osiągnąć za pomocą listy kontrolnej dotyczącej gotowości do eksploatacji.*

### ***Etap eksploatacji i utrzymania***

Organizacja opracowała dokumentację dotyczącą eksploatacji i utrzymania, w której określa się procesy systemu zarządzania bezpieczeństwem wykorzystywane do aktualizacji, przeglądu i utrzymania jej aktywów. Opisuje się w niej zakres działalności i, jeśli jest taka potrzeba, wdrożone strategie zarządzania ryzykiem, które obejmują wszystkie istotne działania.

W tej dokumentacji:

- *zapewnia się, aby aktywa były eksploatowane i utrzymywane zgodnie z tym, jak zostały zaprojektowane;*
- *wskazuje się i uwzględnia wszystkie warunki związane z bezpieczeństwem, które pozwalają określić, jakie mogą być ograniczenia korzystania z danych aktywów, w jakich warunkach będą wykorzystywane; oraz*
- *określa się, jaka bieżąca kontrola ma być prowadzona.*

Proces dotyczący konfiguracji projektowania i przygotowania proponowanych aktywów (opisany na etapie projektu) zostaje rozszerzony tak, aby objął cały cykl życia aktywów za pomocą:

- *utworzenia i utrzymywania zapisów na temat wszystkich aktywów dzięki stworzeniu rejestru aktywów. Uwzględnia to informacje takie jak jednoznaczne oznaczenie aktywów, ich lokalizacja, wszelkie przeprowadzone prace związane z utrzymaniem itp.;*
- *zarządzania dokumentami i informacjami na temat aktywów zgodnie z system zarządzania bezpieczeństwem organizacji (**zob. również 4.4 i 4.5**); oraz*
- *określania istotności aktywów w oparciu o wyniki oceny ryzyka w zakresie bezpieczeństwa. Aktywa o istotnym znaczeniu dla bezpieczeństwa są wskazywane w rejestrze aktywów.*

Organizacja opisuje w swoim dzienniku zagrożeń sposób, w jaki informacje dotyczące aktywów są opracowywane, utrzymywane i włączane.

Organizacja monitoruje ciągłe pozostawanie w zgodności z wyznaczonymi normami i procesami w celu zapewnienia, aby jej działalność kolejowa była w dalszym ciągu bezpieczna i sprawnie funkcjonowała. W tym celu organizacja ustanawia procesy mające na celu zapewnienie, aby:

- *aktywa były eksploatowane i utrzymywane zgodnie z właściwymi instrukcjami;*
- *stan aktywów był monitorowany;*
- *wyposażenie potrzebne do testowania lub inspekcji aktywów było odpowiednio kontrolowane, kalibrowane i utrzymywane;*

- *wszelkim ryzykiem związanym z eksploatacją i utrzymywaniem aktywów zarządzano zgodnie z procesami zarządzania ryzykiem i wszystkimi przepisami dotyczącymi zdrowia i bezpieczeństwa w miejscu pracy; oraz*
- *w ramach działań związanych z utrzymaniem zawsze były dostępne części zamiennie, szczególnie w przypadku aktywów o istotnym znaczeniu dla bezpieczeństwa. Można to osiągnąć poprzez określenie zapotrzebowania na części zamiennie w oparciu o istotność danych aktywów, którą można wskazać poprzez wykorzystanie „utrzymania skupionego na niezawodności” (reliability centred maintenance – RCM).*

Organizacja wykazuje, że posiada plan utrzymania zasobów, aby:

- *odnieść się do wymogów dotyczących predyspozycji, zdolności i zasobów;*
- *zapewnić zarządzanie informacjami i konieczność prowadzenia rejestrów;*
- *dostarczyć szczegółowe plany, które ustanowiono w ramach procesu opartego na analizie ryzyka i które określają poszczególne poziomy utrzymania oraz ustanowione standardowe struktury organizacyjne, procedury i obowiązki związane z utrzymaniem aktywów, oraz*
- *zapewnić kalibrację narzędzi i sprzętu, który zostanie wykorzystany do utrzymania.*

Może to obejmować w szczególności:

- *„Techniczny plan utrzymania” (TMP) oraz*
- *instrukcje służbowe opracowane i poddane audytowi na podstawie Technicznego planu utrzymania.*

Planowanie dokumentuje się i kontroluje, np. stosując komputerowy system zarządzania utrzymaniem (**zob. również 4.5**).

Organizacja posiada procesy mające zapewnić:

- *w przypadku, gdy pojazd lub sprzęt przydzielono do zadania, aby:*
  - *zgodność z zadaniem/misją do wykonania (np. kompatybilność techniczna każdego rodzaju taboru z trasami) była sprawdzana podczas przygotowania i przed rozpoczęciem eksploatacji;*
  - *dokonano utrzymania co najmniej elementów o istotnym znaczeniu dla bezpieczeństwa zgodnie z planem (utrzymanie prewencyjne z uwzględnieniem częstotliwości i rodzaju interwencji);*
  - *określono interwencje związane z utrzymaniem, gdy zidentyfikowano wady lub gdy przekraczają one bezpieczne granice użytkowania (utrzymanie naprawcze), chyba że wdrożono ograniczenia operacyjne;*
  - *po zidentyfikowaniu konieczności zmiany, takiej jak wycofanie z eksploatacji lub ustalenie ograniczeń operacyjnych, jak najszybciej podjęto konieczne działania.*
- *dostępność instrukcji służbowych w odniesieniu do wszystkich działań o istotnym znaczeniu dla bezpieczeństwa;*
- *zakończenie wszystkich zadań w odniesieniu do zgodności z wymogami;*
- *kontrolę dokumentacji dotyczącej przeprowadzonych prac związanych z utrzymaniem (**zob. również 4.5**) oraz*
- *dostępność szkolenia opartego na predyspozycji we wszystkich systemach o istotnym znaczeniu dla bezpieczeństwa (**zob. również 4.1**).*

Istnieje proces/procedura dotyczący(-a) zapewnienia, że ograniczenia operacyjne – tymczasowe lub trwałe (np. związane z określonym rodzajem pojazdu lub określonymi trasami):

- *bierze się pod uwagę, w przypadku gdy pojazd lub sprzęt przydzielono do zadania/misji;*
- *w odpowiednim czasie podaje się do wiadomości personelowi obsługującemu pojazd lub sprzęt (np. maszyniście lub kierownikowi pociągu).*

Organizacja wykazuje że:

- rozumie funkcjonowanie swoich aktywów o istotnym znaczeniu dla bezpieczeństwa poprzez określenie co należy monitorować, zmierzyć i zgłosić;
- ustanawia i rejestruje metodę i częstotliwość monitorowania, pomiaru, analizy i oceny funkcjonowania aktywów o istotnym znaczeniu dla bezpieczeństwa;
- monitoruje tendencję działalności w odniesieniu do przewidywanego życia strategicznego aktywów **(zob. również 6.1)**;
- sporządza sprawozdania na temat kwestii związanych z działalnością w oparciu o poziom ryzyka w zakresie bezpieczeństwa i podnosi kwestie związane ze skutecznością działania w zakresie bezpieczeństwa, tak więc rozwiązuje je w odpowiedni sposób;
- wykorzystuje wyniki monitorowania w celu przyjęcia planu utrzymania w stosownych przypadkach;
- ustanawia kanały, aby podawać do wiadomości wszelkie wyniki **(zob. również 4.4)**;
- poprawia zgodność aktywów o istotnym znaczeniu dla bezpieczeństwa z normami poprzez:
  - przegląd kontroli operacyjnych i kontroli dotyczących utrzymania oraz poprzez ocenianie ryzyka aktywów niespełniających wcześniej określonych norm;
  - identyfikowanie podstawowych przyczyn dotyczących kwestii związanych ze skutecznością działania w zakresie bezpieczeństwa oraz
  - określanie działań, które mogą być konieczne w celu przywrócenia aktywów do bezpiecznych warunków działalności;
- stale usprawnia system zarządzania bezpieczeństwem poprzez identyfikowanie potencjalnego ryzyka i podejmowanie działań naprawczych **(zob. również 7.2)** oraz
- dokumentuje przypadki wykorzystania możliwości ograniczenia lub eliminacji ryzyka oraz sposób, w jaki to osiągnięto.

Organizacja posiada procesy dotyczące identyfikowania błędów lub awarii, które mogą się pojawić w odniesieniu do aktywów oraz zapewniające przeprowadzenie odpowiednich działań naprawczych. Procesy te są zgodne z przepisami i programami lub planami dotyczącymi utrzymania oraz:

- zapewniają odpowiednie rejestrowanie błędów i wynikających z nich działań naprawczych;
- odnoszą się do błędów o istotnym znaczeniu dla bezpieczeństwa;
- zapewniają odpowiednie sporządzanie sprawozdań na temat zdarzeń wymagających zgłoszenia oraz
- koordynują nieplanowane naprawy aktywów związanych z bezpieczeństwem.

Organizacja:

- dokumentuje proces zarządzania błędami;
- stosuje odpowiednie techniki analizy w przypadku cech o istotnym znaczeniu dla bezpieczeństwa, takie jak „Analiza podstawowych przyczyn” (RCA);
- wdraża rejestrowanie błędów, co może obejmować kody błędów, tryb awaryjny, skutek, krytyczność i działania naprawcze;
- opracowuje procedury w celu zarządzania wspólnymi działaniami naprawczymi; oraz
- wprowadza proces przekazywania informacji zwrotnych dla zespołów inżynierskich lub technicznych w celu przeglądu i poprawy systemów i zminimalizowania ryzyka przyszłych awarii.

Osiąga się to poprzez stosowanie sprawozdawczości i analizy błędów oraz działań naprawczych (FRACAS), która:

- rejestruje błędy, które wykryto i zarejestrowano podczas przeprowadzania testów i oddawania do użytku, jak również błędów, które wystąpiły podczas eksploatacji lub utrzymania; oraz
- zarządza późniejszymi działaniami naprawczymi, podjętymi w celu naprawienia tych błędów.

Organizacja dokumentuje wszystkie błędy i działania naprawcze oraz zobowiązuje osobę kompetentną technicznie do skontrolowania wszelkich nieplanowanych napraw.

Istnieje proces/procedura kierująca zarządzaniem w sytuacjach awaryjnych lub kryzysowych dotyczących zarządzania aktywami.

Organizacja ustanowiła procesy w celu zarządzania ryzykiem na wspólnej płaszczyźnie, które występuje podczas eksploatacji i utrzymania jej aktywów (**zob. również 3.1.1**). Dotyczy to wspólnej płaszczyzny między aktywami oraz między podmiotami, które z nich korzystają.

#### ***Etap odnowienia, wycofania z użytku i usunięcia***

Organizacja rozumie stan swoich aktywów i w przypadku jego pogorszenia odpowiada właściwie, zastępując je lub poddając procesowi utrzymania.

Organizacja ustanowiła plan testów dotyczący poświadczania i oddawania do użytku mający na celu potwierdzenie, że nowe aktywa są odpowiednie do celu, a ich eksploatacja i utrzymanie są bezpieczne. Jeśli organizacja przedłuża okres eksploatacji istniejących aktywów, poszukuje informacji dotyczących bezpieczeństwa, takich jak dane historyczne, aby zapewnić ich dalsze bezpieczne stosowanie.

Przeprowadza się monitorowanie tendencji w odniesieniu do oczekiwanej działalności (zob. etap eksploatacji i utrzymania).

W przypadku usuwania jakiegokolwiek infrastruktury kolejowej lub taboru kolejowego organizacja odpowiednio zarządza ryzykiem wycofania aktywów z użytku.

#### ***Zarządzanie zmianami dotyczącymi aktywów o istotnym znaczeniu dla bezpieczeństwa***

W sytuacjach, gdy organizacja dąży do wprowadzenia zmian w podstawowej konfiguracji aktywów o istotnym znaczeniu dla bezpieczeństwa, wdraża proces zarządzania zmianami, aby zapewnić skuteczne zarządzanie ryzykiem dotyczącym bezpieczeństwa, ustanawiając podstawową konfigurację z powiązaniem oprogramowaniem (połączonym w istniejących systemach lub będącym odrębnymi programami) w przypadku wszystkich aktywów o istotnym znaczeniu dla bezpieczeństwa. Jeżeli operator wprowadza zmiany do podstawowej konfiguracji aktywów o istotnym znaczeniu dla bezpieczeństwa, ma w miarę możliwości:

- *zarządzać ryzykiem wynikającym ze zmian tych aktywów;*
- *prowadzić ewidencję numerów seryjnych i numerów modeli;*
- *poświadczać spełnianie funkcjonalnych wymogów względem specyfikacji i środków kontroli ryzyka;*
- *kontrolować dopuszczanie elementów konfiguracyjnych; oraz*
- *zapewniać, aby status wszystkich aktywów w ramach zarządzania konfiguracją był aktualny.*

Zmiany w przyjętych przez organizację wartościach podstawowych, warunkach prowadzenia działalności lub harmonogramach utrzymania aktywów o istotnym znaczeniu dla bezpieczeństwa w żaden sposób nie zmniejszają poziomu bezpieczeństwa działalności kolejowej.

#### ***Stosowanie wspólnych metod oceny bezpieczeństwa***

Istnieje proces lub procedura mające na celu monitorowanie, że podmioty odpowiedzialne za utrzymanie stosują, w stosownych przypadkach, wspólną metodę oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka i wspólną metodę oceny bezpieczeństwa w odniesieniu do monitorowania (tj. wymagane w przepisach lub w ustaleniach umownych).

Uwzględnienie czynników ludzkich i organizacyjnych oraz poprawa kultury bezpieczeństwa będą miały pozytywny wpływ na spełnienie odpowiedniego wymogu systemu zarządzania bezpieczeństwem, a dowody na to można znaleźć w następujących źródłach:

Rejestr zagrożeń organizacji zawierający ryzyka dla bezpieczeństwa związane ze wszystkimi etapami wchodzącymi w skład cyklu życia zarządzania składnikiem majątku oraz identyfikujący podstawowe czynniki ludzkie i organizacyjne związane z podstawowymi przyczynami w przypadku każdego scenariusza ryzyka związanego z zarządzaniem cyklem życia składnika majątku.

W programie organizacji określa się ramy dotyczące sposobu, w jaki rozpoznane ryzyka związane z czynnikami ludzkimi i organizacyjnymi będą przeglądane i uzgadniane i w jaki sposób posunie się je do przodu w celu stworzenia rozwiązań w projekcie lub w procesie zarządzania zmianą. W programie określa się stosunki z innymi stronami związanymi z działalnością dotyczącą projektu lub zmian.

Na przykład:

- *użytkownicy końcowi stanowią część analizy potrzeb, może to obejmować analizy zadań i wywiady, niektórzy przedstawiciele pracowników są zaangażowani od fazy projektowania do fazy testowania;*
- *istnieją procedury i specjalne środki zapewniające jasną komunikację między zespołami operacyjnymi i zespołami ds. utrzymania, a także z podmiotami odpowiedzialnymi za utrzymanie;*
- *użytkownicy końcowi są również zaangażowani w procesy zarządzania zmianami, w tym w automatyzację. Pracownicy mogą przekazywać zespołowi ds. projektów informacje zwrotne, które są analizowane, i podejmowane są działania usprawniające. Protokoły z posiedzeń i sprawozdania z zarządzania zmianami wyraźnie wskazują na ich zaangażowanie i uwzględnienie ich obaw;*
- *wszyscy zainteresowani użytkownicy są identyfikowani w ramach oceny ryzyka, a w ramach systemu zarządzania kompetencjami przeprowadza się dla nich szkolenia, aby zapewnić utrzymanie kompetencji przez pracowników;*
- *producenci i dostawcy są zaangażowani w proces projektowania i zarządzania zmianami w celu zapewnienia odpowiedniego uwzględnienia czynników ludzkich.*

Przedstawiono informacje dotyczące stosowania narzędzia SAIT (**zob. 5.4.3**).

#### 5.2.6 Odniesienia i normy

- [Wytyczne dotyczące podmiotów odpowiedzialnych za utrzymanie](#)
- [Nota wyjaśniająca ERA dotycząca bezpiecznej integracji](#)
- CENELEC – EN50126 Zastosowania kolejowe – Specyfikowanie i wykazywanie niezawodności, dostępności, możliwości utrzymania i bezpieczeństwa (RAMS) Część 1: Wymagania podstawowe i procesy ogólnego przeznaczenia
- [Biuro krajowego organu regulacyjnego ds. bezpieczeństwa kolei \(Office of the National Rail Safety Regulator\) – Wytyczne dotyczące zarządzania aktywami \(2019\)](#)
- ISO 55000:2014 Zarządzanie aktywami – Przegląd, zasady i terminologia
- ISO 55001:2014 Zarządzanie aktywami – Systemy zarządzania – Wymagania

#### 5.2.7 Kwestie związane z nadzorem

Z punktu widzenia nadzoru ważne jest, aby skupiono się na zarządzaniu danymi aktywami przez cały ich cykl życia, od projektu aż po zakończenie użytkowania, a nie na przypadkach nieprawidłowego zarządzania danymi aktywami, chyba że mają bezpośredni wpływ na bezpieczeństwo.

W ramach nadzoru należy brać pod uwagę, w jaki sposób utrzymywane są istniejące aktywa, które powstały przed wprowadzeniem obecnych standardów, oraz w jaki sposób się nimi zarządza.

W ramach nadzoru należy sprawdzić, czy i w jaki sposób organizacja używa SAIT.



## 5.3 Wykonawcy, partnerzy i dostawcy

### 5.3.1 Wymóg regulacyjny

- 5.3.1. Organizacja musi określić i kontrolować ryzyka dla bezpieczeństwa wynikające z działalności zleconej w ramach outsourcingu, w tym z działalności lub współpracy z wykonawcami, partnerami i dostawcami.
- 5.3.2. W celu kontrolowania ryzyk dla bezpieczeństwa, o których mowa w pkt 5.3.1, organizacja musi zdefiniować kryteria wyboru wykonawców, partnerów i dostawców oraz wymogi dotyczące umów, które podmioty te muszą spełniać, w tym:
- (a) wymogi prawne i inne wymogi związane z bezpieczeństwem (zob. pkt 1. Kontekst organizacji);
  - (b) poziom kompetencji wymaganych do realizacji zadań określonych w umowie (zob. pkt 4.2 Kompetencje);
  - (c) odpowiedzialność za wykonywane zadania;
  - (d) oczekiwane wyniki w zakresie bezpieczeństwa, które mają być utrzymywane w trakcie obowiązywania umowy;
  - (e) obowiązki dotyczące wymiany informacji związanych z bezpieczeństwem (zob. pkt 4.4 Informowanie i komunikowanie);
  - (f) identyfikowalność dokumentów dotyczących bezpieczeństwa (zob. pkt 4.5 Dokumentacja).
- 5.3.3. Zgodnie z procesem określonym w art. 3 rozporządzenia (UE) nr 1078/2012 organizacja musi monitorować:
- (a) wyniki w zakresie bezpieczeństwa w przypadku wszystkich działań i operacji wykonawców, partnerów i dostawców, tak aby zapewnić, by spełniały one wymogi określone w umowie;
  - (b) świadomość wykonawców, partnerów i dostawców co do ryzyk dla bezpieczeństwa, jakie niosą one ze sobą w odniesieniu do działalności organizacji.

### 5.3.2 Cel

Wnioskodawca musi wykazać, że posiada zdolność identyfikacji, oceny i kontrolowania zagrożeń, które wynikają z działań prowadzonych przez wykonawców i innych dostawców, z którymi współpracuje. Nie jest to tylko kwestia oceny ryzyka i nie wymaga też wykazu wszystkich zagrożeń lub kategorii istotnych zagrożeń, ale wnioskodawca musi wykazać, że jego systemy i procedury są całościowo zaprojektowane i zorganizowane w celu ułatwienia identyfikacji, oceny i kontrolowania tych zagrożeń. Oznacza to, że umowa musi również zawierać ustalenia dotyczące wymiany informacji w zakresie bezpieczeństwa. Powszechnie stosowanym i akceptowanym sposobem na zarządzanie ryzykiem jest zawieranie dobrze napisanych umów. Główna odpowiedzialność za zarządzanie wykonawcami i za sprawdzanie świadczonych przez nich usług pod kątem zgodności z ustalonymi specyfikacjami spoczywa jednak na organizacji. Korzystanie z usług wykonawców lub podwykonawców nie oznacza, że przedsiębiorstwo kolejowe/ zarządca infrastruktury przenosi jakkolwiek swoją odpowiedzialność dotyczącą zapewnienia, aby zlecone usługi zostały wykonane zgodnie z normami określonymi przed rozpoczęciem działalności.

Wnioskodawca powinien wykazać, że w ramach swojej procedury udzielania zamówień wdrożył procesy mające na celu określenie kompetencji wykonawców i innych dostawców oraz ocenę ich skuteczności działania w zakresie bezpieczeństwa.

Każda organizacja odpowiada za przeprowadzanie procesu monitorowania, który określono we wspólnej metodzie oceny bezpieczeństwa w odniesieniu do monitorowania, oraz zapewnienie monitorowania, poprzez ustalenia umowne, środków kontroli ryzyka wdrożonych przez jej wykonawców, zgodnie ze wspólną metodą oceny bezpieczeństwa. Jeśli organizacje dostrzegą jakiegokolwiek istotne zagrożenie dotyczące bezpieczeństwa związane z usterkami lub awariami sprzętu technicznego, zgodnie z wspólną metodą oceny bezpieczeństwa w odniesieniu do monitorowania mają obowiązek zgłosić te zagrożenia pozostałym zaangażowanym stronom, tak aby mogły podjąć niezbędne działania naprawcze w celu zapewnienia bezpieczeństwa systemu.

### 5.3.3 Noty wyjaśniające

Dodatkowe informacje dotyczące ustaleń umownych i partnerstw można znaleźć w części Załącznik 3.

#### ***Jak uwzględnić czynniki ludzkie i organizacyjne oraz kulturę bezpieczeństwa?***

Określone przez przedsiębiorstwo procesy kontroli ryzyka obejmują działania wykonawców, partnerów i dostawców. Ryzyko i środki bezpieczeństwa określone przez przedsiębiorstwo są komunikowane wykonawcom, dostawcom i partnerom oraz uwzględniane w specyfikacjach w odniesieniu do każdego rodzaju działalności zleconej na zewnątrz. Może to również obejmować monitorowanie wyników działalności zleconej na zewnątrz (zob. sekcja **6.1 Monitorowanie** poniżej).

Strategia dotycząca czynników ludzkich i organizacyjnych może obejmować istotne kwestie dotyczące wykonawców, partnerów i dostawców.

Role, obowiązki i kompetencje niezbędne do realizacji zleconych zadań są jasno określone w umowach. Kompetencje te są takie same, jak te opisane w systemie zarządzania kompetencjami dla pracowników wewnętrznych.

Umowy zawierają postanowienia dotyczące sposobu zarządzania informacjami i komunikacją w zakresie bezpieczeństwa, aby zapewnić ten sam poziom bezpieczeństwa opisany w odniesieniu do informacji i komunikacji wewnętrznej. Dotyczy to również wymiany wiedzy.

### 5.3.4 Dowody

- *Dowody dotyczące sposobu, w jaki system zarządzania bezpieczeństwem współdziała z systemami zarządzania wykonawców i dostawców w celu kontroli ryzyka; **(5.3.1)***
- *dowody potwierdzające, że ustalenia umowne są opracowywane w oparciu o wyniki oceny ryzyka; **(5.3.1) (zob. również 3.1)***
- *istnieją procesy określające, w jaki sposób należy uwzględniać czynniki ludzkie i organizacyjne oraz przekazać te informacje podwykonawcom, a także zarządzać nimi; **(5.3.1)***
- *dowody na temat sposobu, w jaki organizacja zarządza dokumentacją dotyczącą wykonawców i dostawców; **[5.3.2 lit. a)–d)]***
- *dowody opisujące metody stosowane przez organizację do wybierania wykonawców i dostawców przy zapewnieniu, aby byli kompetentni i aby ryzyko związane z bezpieczeństwem było odpowiednio zarządzane; **[5.3.2 lit. a)–e)]***
- *proces wdrożony w celu zapewnienia, aby istotne informacje dotyczące bezpieczeństwa były przekazywane wykonawcom i dostawcom lub przez nich zgłaszane; **[5.3.2 lit. d)]***
- *dowody na to, jak procedura kontroli dokumentów zapewnia zarządzanie dokumentami związanymi z bezpieczeństwem, które są istotne dla wykonawców i dostawców; **[5.3.2 lit. f)]***

- *proces lub procedura monitorowania, które organizacja wdrożyła w celu upewnienia się, że wykonawcy, partnerzy i dostawcy, z którymi utrzymywana jest współpraca, są w stanie kontrolować ryzyko, na które te podmioty są narażone; [5.3.3 lit. a)–b)]*
- *dowody potwierdzające, że wykonawcy, partnerzy lub dostawcy są regularnie monitorowani zgodnie ze wspólną metodą oceny bezpieczeństwa w odniesieniu do monitorowania (rozporządzenie (UE) 1078/2012) w celu zapewnienia, aby dostarczane produkty lub świadczone usługi spełniały określone wymogi i cele w zakresie bezpieczeństwa. [5.3.3 lit. a)] (zob. również 6.1)*

### 5.3.5 Przykłady dowodów

Dowody, że cele w zakresie bezpieczeństwa, których realizacji organizacja oczekuje od wykonawców, partnerów i dostawców, oraz wskaźniki, które zostaną wykorzystane do pomiaru postępów w ich osiągnięciu, zostały im dostarczone.

Procedura zarządzania dokumentami dotycząca norm organizacji, które mają być zastosowane przez wykonawców, partnerów i dostawców (zob. również 4.5.1.1 lit. e) Zarządzanie dokumentami).

Wykaz/przegląd współpracujących z organizacją wykonawców, partnerów i dostawców przeznaczony do wykorzystania wewnętrznego lub zewnętrznego wraz ze specyfikacjami produktów lub usług przez nich dostarczanych lub świadczonych [zob. również 4.5.1.1 lit. d) i e)] oraz wskazanie, jaki jest wpływ na bezpieczeństwo wraz ze środkami mającymi na celu kontrolowanie rozpoznanego ryzyka (np. wymiana informacji, wyjaśnienie obowiązków, szkolenia) [zob. również 3.1.1.1 lit. a)].

Uwzględnienie czynników ludzkich i organizacyjnych oraz poprawa kultury bezpieczeństwa będą miały pozytywny wpływ na spełnienie odpowiedniego wymogu systemu zarządzania bezpieczeństwem, a dowody na to można znaleźć w następujących źródłach:

Odpowiedni proces planowania audytu/inspekcji w odniesieniu do swoich wykonawców, partnerów i dostawców, wraz z kilkoma przykładowymi rejestrami takich działań, takimi jak sprawozdania lub ustalenia z audytu/inspekcji i powiązane plany działań.

Strategia dotycząca czynników ludzkich i organizacyjnych zawiera informacje szczegółowe dotyczące tego, w jaki sposób te kwestie dotyczą wykonawców, partnerów i dostawców.

Procedura, w ramach której wykonawcy, partnerzy i dostawcy są wybierani i monitorowani. Procedura jasno określa, że normy, które mają stosować wykonawcy, są takie same jak te stosowane przez personel zatrudniony bezpośrednio, oraz określa role i obowiązki. W ramach tej procedury dokumentuje się wymianę niezbędnych informacji między systemem zarządzania bezpieczeństwem wnioskodawcy a systemami zarządzania bezpieczeństwem wykonawców, partnerów i dostawców.

Procedura systemu zarządzania kompetencjami, która wiąże się z analogicznymi procedurami wykonawców, partnerów i dostawców współpracujących z organizacją.

Proces lub procedura zarządzania wykonawcami, partnerami i dostawcami obejmujące sposób zarządzania ryzykiem wynikającym z powiązań między działalnością wykonawców, partnerów lub dostawców, sposób wymiany informacji w tym zakresie oraz – w stosownych przypadkach – sposób uwzględniania tego ryzyka w ustaleniach umownych oraz w jaki sposób wymiana informacji jest zintegrowana z systemem zarządzania bezpieczeństwem.

Proces lub procedura, za pośrednictwem której określa się istotne wymogi mające zastosowanie w odniesieniu do wykonawców, partnerów lub dostawców i przekazuje im je do wiadomości, oraz w jaki sposób wymogi te zawarto w ustaleniach umownych, które właściwie udokumentowano w ramach systemu zarządzania dokumentami, aby zapewnić identyfikowalność informacji.

Procedura systemu zarządzania dokumentami dotycząca certyfikatów, zezwoleń, uznań lub wszelkich innych rodzajów dowodów wykazujących zgodność z wymogami mającymi zastosowanie w odniesieniu do wykonawców, partnerów lub dostawców i która kontroluje ich ważność na przestrzeni czasu (np. poprzez działania w zakresie monitorowania).

#### 5.3.6 *Kwestie związane z nadzorem*

W przypadku nadzorowania organizacji, w celu uzyskania pełnego obrazu zakresu kontroli i monitorowania, konieczne może być przeprowadzenie działań nadzorczych z udziałem wykonawcy lub dostawcy pracującego dla tej organizacji. Konieczne może być również uzyskanie dostępu do dokumentacji, na podstawie której wykonawca lub dostawca wykonuje swoją pracę i zbadanie, w jaki sposób odnosi się ona do procedur określonych w systemie zarządzania bezpieczeństwem organizacji.

Ustalenia mające na celu zapewnienie, aby skuteczność działania w zakresie bezpieczeństwa i kompetencja wykonawcy i dostawcy były integralną częścią procedury udzielania zamówień.

## 5.4 Zarządzanie zmianą

### 5.4.1 Wymóg regulacyjny

5.4.1. Organizacja musi wdrażać i kontrolować zmiany w systemie zarządzania bezpieczeństwem w celu utrzymania lub poprawy wyników w zakresie bezpieczeństwa. Obejmuje to podejmowanie decyzji na poszczególnych etapach procesu zarządzania zmianą oraz późniejszy przegląd ryzyk dla bezpieczeństwa (zob. pkt 3.1.1 Ocena ryzyka).

### 5.4.2 Cel

Ważne jest, aby wnioskodawca był w stanie zidentyfikować nowe ryzyko, które może się pojawić w trakcie jego działalności, i odpowiedzieć na nie poprzez zastosowanie w stosownych przypadkach CSM w zakresie wyceny i oceny ryzyka ([rozporządzenie \(UE\) nr 402/2013](#)). System zarządzania bezpieczeństwem powinien wykazać istnienie procedur dotyczących wyceny tego ryzyka i wdrożenia środków kontroli nowego ryzyka, w stosownych przypadkach. Powinno się to odnosić do wszystkich rodzajów i poziomów zmiany – znacznej i nieznacznej, stałej i tymczasowej, natychmiastowej i długoterminowej. Powinno to dotyczyć zmian o charakterze technicznym, operacyjnym lub organizacyjnym.

### 5.4.3 Noty wyjaśniające

Nie wszystkie zmiany podlegają ocenie ryzyka (**5.4.1**). W przypadku gdy zmianami zarządza się aktywnie poprzez inne procesy w systemie zarządzania bezpieczeństwem, takie jak codzienne działania, nie należy ich postrzegać jako zmiany wymagające zarządzania poprzez formalny proces zmiany.

Funkcje, odpowiedzialność, rozliczalność i uprawnienia, które należy określić (**zob. również 2.3**), obejmują zarządzanie zmianą (**5.4.1**), np. przydział funkcji do rady kontroli zmian.

### ***Jak uwzględnić czynniki ludzkie i organizacyjne oraz kulturę bezpieczeństwa?***

Proces zarządzania zmianami umożliwia dokonanie oceny ryzyka w sposób proporcjonalny i kompleksowy, obejmujący w stosownych przypadkach czynniki ludzkie i organizacyjne, oraz umożliwia przyjęcie uzasadnionych środków kontroli.

Podczas przeprowadzania procesu zarządzania zmianami przeprowadza się konsultacje z personelem (**zob. również 2.4**).

Ryzykiem dotyczącym bezpieczeństwa wynikającym z redukcji zatrudnienia lub outsourcingu działań, w tym z działalności lub współpracy z wykonawcami, partnerami i dostawcami, zarządza się – i szereguje je pod względem ważności – jako ryzykiem równym z ryzykiem wewnętrznym.

### 5.4.4 Dowody

- *Opis procesu zarządzania zmianami (**5.4.1**);*
- *opis procedur i metod wykorzystanych do wyceny nowego lub zmienionego ryzyka i wdrożenia nowych (**5.4.1**);*
- *środki kontroli, w tym odniesienia do miejsc, gdzie można znaleźć szczegółowe procesy (**5.4.1**);*
- *informacje na temat sposobu, w jaki organizacja określa znaczne zmiany i decyzje dotyczące tego, kiedy zastosować procesy w zakresie CSM dotyczących wyceny i oceny ryzyka lub kiedy przeprowadzić ocenę ryzyka w ramach procedur systemu zarządzania bezpieczeństwem (**5.4.1**);*

- *informacje na temat ustaleń w ramach zarządzania zmianą, które organizacja podjęła w celu zarządzania zezwoleniami na wprowadzenie pojazdu do obrotu i zmianami dotyczącymi jednolitego certyfikatu bezpieczeństwa lub autoryzacji bezpieczeństwa (5.4.1);*
- *informacje na temat procesu dotyczącego powiadomienia odnośnego krajowego organu ds. bezpieczeństwa o zmianach przed rozpoczęciem nowej operacji transportu kolejowego (5.4.1).*

#### 5.4.5 Przykłady dowodów

Kopia procedury dotyczącej procesu zarządzania zmianami jako część wniosku. Dokument ten obejmuje konieczność przeprowadzenia oceny ryzyka wszystkich zmian zgodnie z odmiennymi wymogami prawnymi. Przykład dziennika istotnych kwestii i założeń, który regularnie poddaje się przeglądowi w miarę dostarczania informacji o postępach zmiany. Ponadto procedura obejmuje również proces, za pośrednictwem którego powiadamia się odnośne krajowe organy ds. bezpieczeństwa o zmianach.

Proces zarządzania zmianą odnosi się do wykorzystania procesu oceny ryzyka, a wyniki są uwzględniane przy opracowywaniu, wdrażaniu i przeglądzie procesów operacyjnych.

Uwzględnienie czynników ludzkich i organizacyjnych oraz poprawa kultury bezpieczeństwa będą miały pozytywny wpływ na spełnienie odpowiedniego wymogu systemu zarządzania bezpieczeństwem, a dowody na to można znaleźć w następujących źródłach:

Zmiany ról, obowiązków, narzędzi i wyposażenia, środowiska pracy, procesów i procedur są wspierane przez analizę czynników ludzkich i organizacyjnych, w ramach której identyfikuje się możliwe ryzyka dla bezpieczeństwa związane z daną zmianą. Stosowane metody to np. analiza zadań, analiza użyteczności, symulacja, ocena ryzyka, HAZOP i badanie bezpieczeństwa. Istnieją przykłady zmian, które powinny być poprzedzone oceną ryzyka z zastosowaniem podejścia opartego na czynnikach ludzkich i organizacyjnych. W szczególności dotyczy to zmiany procedur pracy ze względu na zmodyfikowany sprzęt, zmiany harmonogramów pracy lub ponowny przydział obowiązków.

W przykładach projektów pokazujących, w jaki sposób czynniki ludzkie i organizacyjne zostały uwzględnione w ramach procesu zarządzania zmianą, od samego początku, poprzez analizę potrzeb przedsiębiorstwa: zmiany techniczne, jako nowe urządzenia (sprzęt) lub modernizacje, zmiany organizacyjne lub operacyjne, z oczekiwanym wpływem na istniejącą sytuację itp., dzięki czemu uniknięto nieodpowiedniego projektu, który pogorszyłby wyniki przedsiębiorstwa. Istnieją protokoły ze spotkań analizujące wpływ zmiany na kulturę organizacji oraz sposób, w jaki zostało to zakomunikowane kadrze kierowniczej.

Role i obowiązki w zakresie zarządzania zmianami i związanymi z nimi ryzykami dla bezpieczeństwa są wystarczająco określone, a system zarządzania kompetencjami wskazuje, że osoby odpowiedzialne zostały przeszkolone w zakresie integrowania czynników ludzkich i organizacyjnych.

Dziennik zagrożeń dla projektu tworzony w trakcie realizacji każdego projektu, identyfikujący podstawowe przyczyny związane z czynnikami ludzkimi i organizacyjnymi w odniesieniu do każdego scenariusza ryzyka związanego z bezpieczeństwem. Obejmuje również potencjalny wpływ na wykonawców, partnerów i dostawców, którzy są zaangażowani w razie potrzeby.

Oceny ryzyka dotyczące projektu przeprowadzane są we wczesnych fazach projektu i dotyczą użytkowników końcowych. Ocena ryzyka jest postrzegana jako proces ciągły, który dotyczy bieżących kwestii w trakcie procesu zmian (np. ewolucji założeń i aktualizacji nowo zidentyfikowanych ryzyk).

W ramach procesów/ustaleń administracyjnych między różnymi organizacjami dostarczanie planów i szczegółowych informacji na temat projektu itp. różnym stronom. Związki zawodowe i inne zainteresowane strony są zaangażowane na wczesnym etapie procesu w przypadku wszelkich istotniejszych decyzji lub zmian.

Wykorzystywane narzędzia są takie same jak te przedstawione w rozdziale dotyczącym oceny ryzyka, tj. analiza zadań, analiza użyteczności, symulacja, ocena ryzyka, HAZOP, badanie bezpieczeństwa.

#### 5.4.6 *Kwestie związane z nadzorem*

Aby określić, czy ustalenia w systemie zarządzania bezpieczeństwem dotyczące zarządzania zmianą są wystarczająco solidne, konieczne będzie zastosowanie szeregu różnego rodzaju zmian poprzez określony proces, aby sprawdzić czy a) odpowiednio nimi zarządzono i czy właściwie uwzględniono ryzyko wynikające ze zmian i b) czy wyciągnięte wnioski włączono do zmian procedur systemu zarządzania bezpieczeństwem.

Ocenienie zgodności ustaleń dotyczących zarządzania zmianą ze *wspólną metodą oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka*.

Organizacja posiada procesy dotyczące wdrożenia, stałego monitorowania odnośnych TSI, przepisów krajowych i innych norm, w stosownych przypadkach pokazujące, w jaki sposób zastosowano je w całym cyklu życia każdego sprzętu lub działalności.

## 5.5 Zarządzanie sytuacjami kryzysowymi

### 5.5.1 Wymóg regulacyjny

- 5.5.1. Organizacja identyfikuje sytuacje kryzysowe oraz powiązane środki, które należy terminowo przedsięwziąć w celu zarządzania tymi sytuacjami (zob. pkt 3.1.1 Ocena ryzyka) i przywrócenia normalnych warunków prowadzenia działalności zgodnie z rozporządzeniem (UE) 2015/995.
- 5.5.2. W odniesieniu do każdego zidentyfikowanego rodzaju sytuacji kryzysowej organizacja zapewnia:
- (a) możliwość natychmiastowego kontaktu ze służbami ratowniczymi;
  - (b) przekazanie służbom ratowniczym wszystkich ważnych informacji zarówno z wyprzedzeniem, w celu przygotowania reakcji na sytuację kryzysową, jak i w czasie wystąpienia sytuacji kryzysowej;
  - (c) udzielenie pierwszej pomocy przy użyciu zasobów wewnętrznych.
- 5.5.3. Organizacja określa i dokumentuje funkcje i obowiązki wszystkich stron zgodnie z rozporządzeniem (UE) 2015/995.
- 5.5.4. Organizacja posiada plany działania, procedury alarmowe oraz informacje na wypadek wystąpienia sytuacji kryzysowej, które obejmują ustalenia dotyczące:
- (a) alarmowania wszystkich pracowników odpowiedzialnych za zarządzanie w sytuacjach kryzysowych;
  - (b) przekazywania informacji wszystkim stronom (np. zarządcom infrastruktury, przedsiębiorstwom kolejowym, wykonawcom, organom, służbom ratowniczym), w tym instrukcji postępowania w sytuacjach kryzysowych dla pasażerów;
  - (c) podejmowania wszelkich decyzji wymaganych zgodnie z rodzajem sytuacji kryzysowej.
- 5.5.5. Organizacja musi opisać sposób podziału zasobów i środków na potrzeby zarządzania w sytuacji kryzysowej (zob. pkt 4.1 Zasoby) oraz sposób określenia wymogów szkoleniowych (zob. pkt 4.2 Kompetencje).
- 5.5.6. Ustalenia dotyczące sytuacji kryzysowych są okresowo testowane we współpracy z innymi zainteresowanymi stronami oraz w stosownych przypadkach aktualizowane.
- 5.5.7. Organizacja musi zapewnić zarządcy infrastruktury możliwość łatwego i niezwłocznego kontaktu z właściwymi kompetentnymi pracownikami z odpowiednią znajomością języków, jak również zapewnić mu odpowiednie informacje.
- 5.5.7. Organizacja musi koordynować plany na wypadek sytuacji kryzysowych ze wszystkimi przedsiębiorstwami kolejowymi prowadzącymi działalność z wykorzystaniem infrastruktury organizacji, ze służbami ratunkowymi, tak aby ułatwić ich szybką interwencję, a także ze wszystkimi innymi stronami, które mogłyby być zaangażowane w sytuację kryzysową.
- 5.5.8. Istnieje procedura na potrzeby skontaktowania się w sytuacji kryzysowej z podmiotem odpowiedzialnym za utrzymanie lub dysponentem pojazdu kolejowego.
- 5.5.8. Organizacja posiada mechanizmy niezwłocznego zatrzymywania eksploatacji i ruchu kolejowego w razie potrzeby oraz informowania wszystkich zainteresowanych stron o podjętych działaniach.
- 5.5.9. W przypadku infrastruktury transgranicznej współpraca między właściwymi zarządcami infrastruktury musi ułatwiać niezbędną koordynację i gotowość właściwych służb ratunkowych po obydwu stronach granicy.



### 5.5.2 Cel

Solidne systemy dotyczące planowania kryzysowego są kluczowe dla każdego podmiotu, na którym spoczywa odpowiedzialność i powinny obejmować informacje, które należy przekazać służbom ratowniczym, aby umożliwić im opracowanie głównych planów reagowania na incydenty. Ważne są również te aspekty systemu zarządzania bezpieczeństwem, które w bezpośredni sposób dotyczą ustaleń w zakresie reagowania kryzysowego, np. szkolenia w zakresie sytuacji kryzysowych i testowanie planów postępowania w sytuacjach kryzysowych.

### 5.5.3 Noty wyjaśniające

Sytuacje kryzysowe (**5.5.1**) wiążą się z wynikami oceny ryzyka przeprowadzonej w organizacji, chociaż TSI OPE (zob. punkt 4.2.3.7) zapewniają nieograniczony wykaz sytuacji kryzysowych.

Pierwsza pomoc udzielana na szczeblu wewnętrznym [**5.5.4 lit. c**] oznacza, że przedsiębiorstwo jest w stanie zarządzać udzielaniem pierwszej pomocy w sytuacjach kryzysowych określonych w pkt 5.5.1.

**Punkty 5.5.7 i 5.5.8** wymogu regulacyjnego zamieszczonego powyżej zaznaczone na niebiesko odnoszą się do zarządcy infrastruktury. **Punkt 5.5.9** powyżej zaznaczony na niebiesko odnosi się tylko do zarządcy infrastruktury.

### **Jak uwzględnić czynniki ludzkie i organizacyjne oraz kulturę bezpieczeństwa?**

Zarządzanie sytuacjami kryzysowymi jest powiązane z zarządzaniem zasobami, rolami i obowiązkami oraz systemem zarządzania kompetencjami w celu zapewnienia świadomości i szkolenia pracowników (w tym utrzymania kompetencji). Obejmuje to rozwój kompetencji (w tym umiejętności innych niż techniczne, takich jak odporność na stres, elastyczność...) dla podmiotów zaangażowanych w plany i procedury na wypadek sytuacji kryzysowych.

### 5.5.4 Dowody

Oczekuje się, że wnioskodawca przedstawi przegląd:

- *rodzajów sytuacji wyjątkowych, które uwzględniono, w tym sytuacji awaryjnych i istniejących procedur do zarządzania nimi (5.5.1);*
- *informacji dostarczonych przez wnioskodawcę, aby umożliwić zaplanowanie służbom ratowniczym odpowiedzi na poważny wypadek na kolei, w stosownych przypadkach odnoszących się do obowiązków zgodnych z przepisami UE mającymi zastosowanie i wszelkimi odnośnymi ustaleniami transgranicznymi [5.5.2 lit. a) i b)];*
- *oczekuje się, że przedsiębiorstwa określą w ramach oceny ryzyka, jaką pierwszą pomoc mogą udzielić same, a jaka musiałaby być udzielona przez służby ratownicze [5.5.2 lit. c)];*
- *planów, funkcji, odpowiedzialności (w tym w przypadku osób o wyznaczonych umiejętnościach przydzielonych do pomocy zarządcy infrastruktury lub odwrotnie); szkoleń i ustaleń w celu utrzymania kompetencji oraz ustaleń dotyczących skutecznej komunikacji ze służbami ratowniczymi, odpowiednim personelem i komunikacji z osobami, których dotyczą incydenty, takimi jak pasażerowie lub strony trzecie dotknięte zdarzeniem (powinno to obejmować dokument, w którym określono funkcje i odpowiedzialność wszystkich stron, sposób, w jaki przydzielono zasoby i środki oraz zidentyfikowano wymogi w zakresie szkoleń); procedury powrotu to zwykłej działalności po wystąpieniu sytuacji kryzysowej (5.5.1), (5.5.3), [5.5.4 lit. a)–c)], (5.5.5), (5.5.7) (5.5.8 i 5.5.9, dotyczy wyłącznie wymogów regulacyjnych spoczywających na zarządcy infrastruktury);*

- *tych konkretnych aspektów systemu zarządzania bezpieczeństwem, które mają bezpośredni związek z ustaleniami w zakresie reagowania kryzysowego, np. szkoleń w zakresie sytuacji kryzysowych i testowania planów postępowania w sytuacjach kryzysowych w celu wykrycia wszelkich słabych punktów (5.5.6);*
- *procedury na potrzeby skontaktowania się z podmiotem odpowiedzialnym za utrzymanie lub dysponentem w sytuacji kryzysowej, która dotyczy jednego z ich pojazdów; (5.5.8, dotyczy wyłącznie wymogów regulacyjnych spoczywających na przedsiębiorstwie kolejowym).*

#### 5.5.5 Przykłady dowodów

Kopia procedury lub procedur zarządzania w sytuacjach kryzysowych oraz powiązanych z nimi planów (np. procedur powrotu do normalnego funkcjonowania). Procedura obejmuje całą sieć, w której prowadzona jest działalność, i uwzględnia, stosownie do potrzeb, konkretne ustalenia dotyczące tuneli i innych miejsc wysokiego ryzyka, ustalenia dotyczące współpracy transgranicznej, polityki kadrowej, ról i obowiązków, a także zawiera odniesienia do ustaleń dotyczących sytuacji kryzysowych stosowanych przez zarządcę infrastruktury oraz metodę kontaktowania się, w stosownych przypadkach, z innymi zainteresowanymi stronami, takimi jak podmiot odpowiedzialny za utrzymanie. W przypadku gdy przedsiębiorstwo kolejowe prowadzi przewozy na infrastrukturze zarządzanej przez różnych zarządców infrastruktury, powinno ono wziąć pod uwagę różnice między ustaleniami dotyczącymi sytuacji kryzysowych (i umowami z użytkownikami) z tymi zarządcami.

Procedura dotycząca sytuacji kryzysowych obejmuje proces, dzięki któremu ofiary incydentów i ich rodziny otrzymują informacje na temat procedur dotyczących skarg.

Procedura (stosownie do potrzeb) uwzględnia informacje na temat tego, co się dzieje w sytuacji kryzysowej z udziałem ładunków niebezpiecznych, a organizacja (przedsiębiorstwo kolejowe) posiada proces mający na celu zapewnienie, aby:

- *istniała możliwość szybkiego kontaktu z załadowcą, właścicielem prywatnej cysterny kolejowej, właścicielem lub dysponentem i operatorem w przypadku kontenera-cysterny, odbiorcą itp.;*
- *jak najszybciej dostarcza się zarządcy infrastruktury istotne informacje (np. numer rejestracji wagonów, pozycja wagonów w pociągu, numer UN, kod klasyfikacyjny RID i numer identyfikacyjny zagrożenia zgodnie z przepisami regulaminu RID);*
- *organizacja (zarządca infrastruktury) wdrożył proces mający na celu zapewnienie, aby organy (np. służby ratownicze, policja, inne służby ratunkowe i inne organy) miały dostęp do istotnych informacji na temat ładunków niebezpiecznych (zob. przykłady powyżej).*

Uwzględnienie czynników ludzkich i organizacyjnych oraz poprawa kultury bezpieczeństwa będą miały pozytywny wpływ na spełnienie odpowiedniego wymogu systemu zarządzania bezpieczeństwem, a dowody na to można znaleźć w następujących źródłach:

Procedura ustalająca scenariusze zidentyfikowanych potencjalnych sytuacji kryzysowych, oceniająca ryzyko związane z poszczególnymi sytuacjami (ze zidentyfikowanymi interfejsami), w tym wynikające z czynników ludzkich i organizacyjnych. Środki bezpieczeństwa zidentyfikowane w celu złagodzenia tych zagrożeń są włączone do odpowiednich planów, procesów i procedur (w tym procedur operacyjnych).

Procedury opisujące związek między planowaniem kryzysowym a zarządzaniem ryzykiem.

Odesłanie w procedurze do wymogów dotyczących systemu zarządzania kompetencjami, jakie mają spełniać pracownicy, których obowiązkiem jest reagowanie na sytuacje kryzysowe, oraz wymóg uzyskania pewności, że zakontraktowani pracownicy są w stanie spełnić te same normy.

Istnieje procedura opisująca zarządzanie ćwiczeniami na wypadek sytuacji kryzysowej (teoretycznymi i praktycznymi) przeprowadzanymi regularnie z udziałem wszystkich zainteresowanych stron (zarówno

wewnętrznych, jak i zewnętrznych), sposób gromadzenia informacji zwrotnych z ćwiczeń na wypadek sytuacji kryzysowych za pomocą działań monitorujących (zob. Sekcja **6.1 Monitorowanie** poniżej) w celu podjęcia działań/środków, mających na celu poprawę planów i procedur postępowania w sytuacjach kryzysowych oraz kompetencji wszystkich zainteresowanych podmiotów (zob. **7.2. Ciągłe doskonalenie** poniżej).

Istnieje procedura zawierająca informacje na temat tego, w jaki sposób ćwiczenia awaryjne są wykorzystywane do zarządzania kompetencjami i usprawniania procesu.

Istnieje procedura opisująca zarządzanie ciągłością działania, którą należy wprowadzić w celu uniknięcia odchyżeń od norm/procedur w przypadku narażenia na nieoczekiwany wpływ na działalność.

Istnieje procedura opisująca sposób wprowadzania planów postępowania w sytuacjach kryzysowych, aby zapewnić skuteczną i szybką interwencję w celu ratowania życia po wypadku.

Przepisy gwarantujące pracownikom organizacji i służbom ratowniczym łatwy dostęp do dokumentacji związanej z planami postępowania w sytuacjach kryzysowych i planami ciągłości działania, aby uniknąć dalszego pogorszenia sytuacji.

Istnieje procedura opisująca, w jaki sposób zalecenia wyrażone przez inne strony (władze, służby ratownicze) oraz najlepsze praktyki są uwzględniane podczas przeglądu planów i procedur postępowania w sytuacjach kryzysowych.

#### 5.5.6 *Kwestie związane z nadzorem*

Aby właściwie ocenić zawarte w systemie zarządzania bezpieczeństwem procedury dotyczące zarządzania sytuacjami wyjątkowymi, konieczne może być krzyżowe zestawienie procedur systemu zarządzania bezpieczeństwem z analogicznymi procedurami stosowanymi przez odpowiednie podmioty, które znajdują się na płaszczyźnie oddziaływań (szczególnie stosunki między najważniejszymi głównymi stronami, takimi jak przedsiębiorstwo kolejowe, zarządca infrastruktury i służby ratunkowe), w celu zapewnienia, aby procesy wdrożone w celu zarządzania takimi incydentami stanowiły spójną całość.

Należy się upewnić, że wdrożono plany na wypadek wszystkich przewidywalnych sytuacji kryzysowych.

Ustalenia dotyczące testowania planów postępowania w sytuacjach kryzysowych oraz skoordynowane ustalenia ze służbami ratunkowymi, które nie są ograniczone do ćwiczeń symulacyjnych.

Ustalenia dotyczące płaszczyzny oddziaływań z innymi zainteresowanymi stronami istnieją i uwzględniają testowanie kontroli, komunikacji, koordynacji i kompetencji.

Usprawnianie funkcjonowania  
systemu kolejowego  
na rzecz społeczeństwa.

## 6 Ocena wyników

### 6.1 Monitorowanie

#### 6.1.1 Wymóg regulacyjny

- 6.1.1. Zgodnie z rozporządzeniem (UE) nr 1078/2012 organizacja prowadzi monitorowanie w celu:
- (a) kontroli prawidłowego stosowania i skuteczności wszystkich procesów i procedur w ramach systemu zarządzania bezpieczeństwem, w tym operacyjnych, organizacyjnych i technicznych środków bezpieczeństwa;
  - (b) kontroli prawidłowego stosowania systemu zarządzania bezpieczeństwem jako całości oraz kontroli tego, czy jego stosowanie przynosi oczekiwane wyniki;
  - (c) zbadania, czy system zarządzania bezpieczeństwem spełnia wymogi niniejszego rozporządzenia;
  - (d) określenia, wdrożenia i oceny skuteczności środków naprawczych (zob. pkt 7.2 Ciągłe doskonalenie), stosownie do sytuacji, w razie wykrycia jakiegokolwiek istotnego przypadku niezgodności z przepisami lit. a), b) i c).
- 6.1.2. Organizacja musi regularnie monitorować na wszystkich poziomach organizacji wyniki realizacji zadań związanych z bezpieczeństwem oraz interweniować, jeżeli zadania te nie są realizowane prawidłowo.

#### 6.1.2 Cel

Organizacja powinna przedstawić dowody na to, że wdrożyła proces monitorowania stosowania i skuteczności systemu zarządzania bezpieczeństwem oraz na to, że ten proces jest właściwy względem rozmiaru, zakresu i rodzaju jej działalności. Organizacja powinna wykazać, że za pomocą tego procesu można rozpoznać, ocenić i naprawić wszelkie wady w funkcjonowaniu systemu zarządzania bezpieczeństwem.

#### 6.1.3 Noty wyjaśniające

Skuteczność środków kontroli oznacza, że organizacja wdrożyła proces, który pozwoli się upewnić, że po przeprowadzeniu oceny ryzyka i zastosowaniu odpowiednich środków kontroli zostaje po jakimś czasie przeprowadzony przegląd tych działań w celu zapewnienia osiągnięcia oczekiwanej w ich efekcie redukcji ryzyka [6.1.1 lit. d)].

#### **Jak uwzględnić czynniki ludzkie i organizacyjne oraz kulturę bezpieczeństwa?**

Regularnie przeprowadza się samokrytyczne i obiektywne oceny programów, praktyk i funkcjonowania, które są związane z kulturą bezpieczeństwa w organizacji. Informacje dotyczące bezpieczeństwa pochodzące na przykład z programu działań naprawczych, analiz działalności człowieka, incydentów i wypadków, badań i istotnych wewnętrznych i zewnętrznych doświadczeń są systematycznie gromadzone i oceniane w celu

zidentyfikowania trendów i uniknięcia organizacyjnego i osobistego dryfowania lub popadania w samozadowolenie.

Dzięki skutecznej ocenie można uzyskać dane pomagające usprawnić skuteczność działania w zakresie bezpieczeństwa poprzez przedstawienie jasnej wizji dotyczącej sposobu, jak kultura bezpieczeństwa organizacji wpływa na bezpieczeństwo. Celem oceny jest wskazanie mocnych i słabych stron kultury bezpieczeństwa poprzez porównanie tego, czym kultura jest, z tym, czym ma być. Umożliwia to wyznaczanie priorytetów w kwestii obszarów, które powinny zostać poprawione, oraz wprowadzenia zmian do, na przykład, procesów, szkoleń i postępowania. Ocena kultury bezpieczeństwa służy proaktywnej pracy nad usprawnianiem skuteczności działania w zakresie bezpieczeństwa oraz zwiększenia marginesów bezpieczeństwa. Zaleca się przeprowadzanie niezależnych ocen kultury bezpieczeństwa co trzy do pięciu lat, a organizacyjnej oceny własnej – corocznie lub co drugi rok.

#### 6.1.4 Dowody

- *Informacje na temat tego, jak wnioskodawca wdrożył wspólną metodę oceny bezpieczeństwa w odniesieniu do monitorowania ([rozporządzenie \(UE\) nr 1078/2012](#)); [6.1.1 lit. a)]*
- *informacje dotyczące sposobu, w jaki rozpoznaje się w ramach procesu monitorowania sukces – lub inny rezultat – w osiąganiu oczekiwanych wyników w zakresie bezpieczeństwa; [6.1.1 lit. b)]*
- *dowody na to, że w systemie zarządzania bezpieczeństwem wprowadzono zmiany, które były efektem naprawiania wad w procesach systemu zarządzania bezpieczeństwem wykrytych w trakcie monitorowania; [6.1.1 lit. c)]*
- *dowody na to, że dokonano przeglądu skuteczności środków naprawczych wprowadzonych w następstwie dowodów na niezgodność z procesami w ramach systemu zarządzania bezpieczeństwem; [6.1.1 lit. d)]*
- *organizacja powinna posiadać proces ustalania norm funkcjonowania i wskaźników dotyczących monitorowania związanego z procesami operacyjnymi oraz wdrożonych zmian. Powinien istnieć program ciągłego oceniania skuteczności procesów związanych z czynnikami ludzkimi i organizacyjnymi oraz oceniania rezultatów tych procesów, np. tego, czy pracownicy postępują zgodnie z wdrożonymi procedurami, a także wykorzystania nowego sprzętu. (6.1.2)*
- *Skuteczność działania w zakresie bezpieczeństwa jest oceniana systematycznie, w świetle strategii dotyczącej poprawy kultury bezpieczeństwa. Oznacza to, że organizacja powinna sprawdzić, w jaki sposób poprawa kultury bezpieczeństwa wpisuje się w cel poprawy bezpieczeństwa i jest jego częścią. (6.1.2)*

#### 6.1.5 Przykłady dowodów

Deklaracja, że wspólna metoda oceny bezpieczeństwa w odniesieniu do monitorowania ([rozporządzenie \(UE\) nr 1078/2012](#)) jest stosowana i że istnieje procedura, która obejmuje te działania. Procedura opisuje szczegółowo, w jaki sposób wyniki w zakresie celów bezpieczeństwa są mierzone i poprawiane poprzez zarządzanie zmianą i proces oceny ryzyka i jak będą poprawiane wady w systemie zarządzania bezpieczeństwem.

Uwzględnienie czynników ludzkich i organizacyjnych oraz poprawa kultury bezpieczeństwa będą miały pozytywny wpływ na spełnienie odpowiedniego wymogu systemu zarządzania bezpieczeństwem, a dowody na to można znaleźć w następujących źródłach:

Organizacja posiadająca procesy i procedury do systematycznej oceny, czy ustalenia dotyczące uwzględnienia czynników ludzkich i organizacyjnych są odpowiednie i czy osiągnięte wyniki są zgodne z normami działalności.

Organizacja posiadająca procesy i procedury do systematycznej oceny wyników personelu z zadań służbowych o istotnym znaczeniu dla bezpieczeństwa. Procesy te opierają się na podejściu proaktywnym, określającym normy dla działalności i systematycznej oceny. Stosuje się metody oparte na dowodach, np. zarządzanie zasobami załogi.

Proces monitorowania, w tym przepisy dotyczące przydzielonych zasobów, w tym personelu i kompetencji pracowników zaangażowanych w działania monitorujące.

Podjęte monitorowanie uwzględnia sprawdzenie wdrożenia i skuteczności procesów i procedur, w ramach których uwzględnia się środki bezpieczeństwa w zakresie czynników ludzkich i organizacyjnych wynikające z procesu oceny ryzyka. W związku z tym w ramach monitoringu uwzględnia się konkretne pozycje dotyczące czynników ludzkich i organizacyjnych, w tym w działaniach operacyjnych. Obejmuje to również ocenę i utrzymanie kompetencji (umiejętności technicznych i pozatechnicznych, postaw, zachowań...) dla personelu (wewnętrznego lub zewnętrznego) wykonującego zadania związane z bezpieczeństwem (zob. sekcja **4.2 Kompetencje** powyżej).

Przeprowadzane monitorowanie uwzględniające analizę sukcesu strategii dotyczącej czynników ludzkich i organizacyjnych.

Proces monitorowania, w tym analiza zgłoszeń pracowników. System zarządzania bezpieczeństwem obejmuje proces oparty na zasadzie „just culture”, w ramach którego karane są rażące zaniedbania, umyślne naruszenia i działania destrukcyjne. Celem jest stworzenie kultury zgłaszania, w której pracownicy czują się swobodnie, ponieważ nie będą obwiniani za niezawinione błędy lub zaniechania. Wyjaśnia to również, w jaki sposób kwestie/incydenty związane z bezpieczeństwem mogą być zgłaszane przez członków personelu, wykonawców lub inne odpowiednie zainteresowane strony.

Proces monitorowania będący elementem doskonalenia organizacyjnego uczenia się. Analiza zgłoszeń pracowników jest analizowana w ramach procesu monitorowania w celu poprawy środków bezpieczeństwa oraz procesów i procedur systemu zarządzania bezpieczeństwem.

Wyniki monitorowania są analizowane z punktu widzenia kultury bezpieczeństwa i włączane do procesu oceny kultury bezpieczeństwa.

#### 6.1.6 Odniesienia i normy

- [Przewodnik dotyczący stosowania wspólnej metody oceny bezpieczeństwa w odniesieniu do monitorowania](#)

#### 6.1.7 Kwestie związane z nadzorem

Badanie procesów monitorujących oraz wynikających z niego ustaleń i działań ma istotne znaczenie dla określenia, czy system zarządzania bezpieczeństwem to „żyjący” i rozwijający się dokument, bowiem doświadczenie generuje poprawę, czy jest to stały dokument, który nie zmienia się w miarę upływu czasu.

Badanie szeregu kluczowych obszarów występowania ryzyka oraz kontroli i przeprowadzanie testów sprawdzających skuteczne stosowanie tych kontroli poprzez system zarządzania bezpieczeństwem ma istotne znaczenie, tak aby krajowy organ ds. bezpieczeństwa mógł ustalić zgodność z wspólną metodą oceny bezpieczeństwa w odniesieniu do monitorowania.

## 6.2 Audyt wewnętrzny

### 6.2.1 Wymóg regulacyjny

- 6.2.1. Organizacja musi przeprowadzać audyty wewnętrzne w sposób niezależny, bezstronny i przejrzysty, tak aby gromadzić i analizować informacje na potrzeby swoich działań w zakresie monitorowania (zob. pkt 6.1 Monitorowanie), obejmujący:
- (a) harmonogram planowanych audytów wewnętrznych, który można modyfikować w zależności od wyników poprzednich audytów i monitorowania wyników;
  - (b) identyfikację i wybór audytorów o odpowiednich kompetencjach (zob. pkt 4.2 Kompetencje);
  - (c) analizę i ocenę wyników audytów;
  - (d) określenie konieczności zastosowania środków naprawczych lub doskonalących;
  - (e) weryfikację wdrożenia i skuteczności tych środków;
  - (f) dokumentację dotyczącą wykonania i wyników audytów;
  - (g) przekazywanie wyników audytów kadrze kierowniczej wyższego szczebla.

### 6.2.2 Cel

Wnioskodawca powinien wykazać, że posiada system audytu wewnętrznego, który obejmuje kompetentny personel i daje wyniki, które kierownictwo uwzględni, oraz zapewnia zgodność systemu zarządzania bezpieczeństwem z przepisami prawnymi.

### 6.2.3 Noty wyjaśniające

Audyty wewnętrzne (**6.2.1**) są narzędziami monitorowania w rozumieniu wspólnej metody oceny bezpieczeństwa w odniesieniu do monitorowania ([rozporządzenie \(UE\) nr 1078/2012](#)). Chociaż jest to osobny wymóg, ma on przyczynić się do osiągnięcia celów monitorowania zgodnie ze wspólną metodą oceny bezpieczeństwa w odniesieniu do monitorowania.

Audyty wewnętrzne (**6.2.1**) mają na celu dostarczenie informacji na temat tego, czy system zarządzania bezpieczeństwem jest zgodny z obowiązującymi wymogami [**6.1.1 lit. c**] i czy jest skutecznie wdrożony i utrzymany [**6.1.1 lit. a), b) i d)**]. Obowiązujące wymogi odnoszą się do wymogów określonych w załączniku I (lub załączniku II) do [rozporządzenia \(UE\) 2018/762](#) i tym samym do wszystkich pozostałych wymogów, do przestrzegania których zobowiązała się organizacja (**zob. również 1.1**).

Audytorzy mają obowiązek weryfikować realizację i skuteczność środków naprawczych lub środków służących poprawie [**6.2.1 lit. c**], które należy podjąć, aby odnieść się do ustaleń audytu.

### 6.2.4 Dowody

- Dowody na istnienie procesu lub ram przeprowadzania audytu wewnętrznego, które przewidują planowane audyty i dodatkowe ukierunkowane audyty w odpowiedzi na dane dotyczące skuteczności działania w zakresie bezpieczeństwa [**6.2.1 lit. a**];
- dowody na istnienie systemu zarządzania kompetencjami, który obejmuje elementy odnoszące się do kompetencji audytorów wewnętrznych [**6.2.1 lit. b**];
- dowody dotyczące ustaleń audytów zarówno wewnętrznych, jak i zewnętrznych, w związku z którymi podjęto działania [**6.2.1 lit. c), d), e), f**];

- *dowody na to, że wyniki audytów omówiono na poziomie kadry kierowniczej wyższego szczebla, w wyniku czego podjęto odpowiednie działania [6.2.1 lit. g)].*

#### 6.2.5 Przykłady dowodów

Istnieje procedura audytu wewnętrznego dotycząca planowanych i dodatkowych audytów, w tym omówienia wyników na poziomie kadry kierowniczej wyższego szczebla.

Przykłady sprawozdań z audytów i dziennik ustaleń z audytów wewnętrznych, w którym wskazano akcje podjęte w celu odniesienia się do tych ustaleń.

Wyniki przeprowadzonych w całej organizacji czynności audytowych są gromadzone, analizowane i wydawane są zalecenia, które mają być zastosowane w związku z okresowym przeglądem dokonywanym przez kierownictwo.

Procedura zawiera odniesienia do systemu zarządzania kompetencjami. CSM wykazuje, że audytorzy postępowali zgodnie z odpowiednim szkoleniem audytorów (np. ISO).

Uwzględnienie czynników ludzkich i organizacyjnych oraz poprawa kultury bezpieczeństwa będą miały pozytywny wpływ na spełnienie odpowiedniego wymogu systemu zarządzania bezpieczeństwem, a dowody na to można znaleźć w następujących źródłach:

Proces audytu wewnętrznego, w tym przepisy dotyczące przydzielonych zasobów, w tym personelu i kompetencji zaangażowanych pracowników. Wymogi dotyczące kompetencji dla pracowników przeprowadzających audyty wewnętrzne są zintegrowane z systemem zarządzania kompetencjami, w tym w zakresie określonych kompetencji dotyczących czynników ludzkich i organizacyjnych. Przykłady szkoleń pokazują, że uwzględniono czynniki ludzkie i organizacyjne.

Audyt wewnętrzny uwzględnia sprawdzenie wdrożenia i skuteczności procesów i procedur, w ramach których uwzględnia się środki bezpieczeństwa w zakresie czynników ludzkich i organizacyjnych wynikające z procesu oceny ryzyka (zob. **6.1 Monitoring** powyżej).

Organizacja posiadająca procesy i procedury systematycznego włączania czynników ludzkich i organizacyjnych do swoich audytów wewnętrznych. Celem jest sprawdzenie skuteczności środków bezpieczeństwa w zakresie czynników ludzkich i organizacyjnych oraz ocena osiągnięcia celów bezpieczeństwa z uwzględnieniem czynników ludzkich i organizacyjnych.

Przykłady audytów wewnętrznych świadczące o uwzględnianiu czynników ludzkich i organizacyjnych podczas analizy wyników audytów, określania potrzeby działań naprawczych lub doskonalących oraz przekazywania ich kadrze kierowniczej wyższego szczebla.

Organizacja posiadająca procesy i procedury do systematycznego włączania oceny wyników personelu wykonującego zadania służbowe o istotnym znaczeniu dla bezpieczeństwa i działania operacyjne.

Proces opisujący zarządzanie komunikacją dotyczącą wyników, zaleceń/środków, co wskazuje na wspólne i przejrzyste podejście.

#### 6.2.6 Odniesienia i normy

- *ISO 19011:2018 – Wytyczne dotyczące audytowania systemów zarządzania*
- [Przewodnik dotyczący stosowania wspólnej metody oceny bezpieczeństwa w odniesieniu do monitorowania](#)



### 6.2.7 *Kwestie związane z nadzorem*

Podczas przeprowadzania nadzoru niezbędne jest przeanalizowanie planowania i ustaleń audytu. Ujawni to, czy audyty ukierunkowane są na właściwe obszary, czy wyniki są uzasadnione i czy personel przeprowadzający audyty jest kompetentny i niezależny.

Należy się upewnić, że obszary wybrane do audytu odpowiadają profilowi ryzyka organizacji.

Istnieje mechanizm służący do inicjowania nieplanowanych audytów i jest stosowany poprzez dokonywanie przeglądu szeregu przykładów.

## 6.3 Przegląd dokonywany przez kierownictwo

### 6.3.1 Wymóg regulacyjny

- 6.3.1. Kadra kierownicza wyższego szczebla musi dokonywać okresowych przeglądów stałej adekwatności i skuteczności systemu zarządzania bezpieczeństwem, obejmujących uwzględnienie co najmniej:
- (a) szczegółowych informacji na temat postępów w zakresie realizacji niewdrożonych jeszcze działań zidentyfikowanych w następstwie poprzednich przeglądów dokonywanych przez kierownictwo;
  - (b) zmieniających się uwarunkowań wewnętrznych i zewnętrznych (zob. pkt 1. Kontekst organizacji);
  - (c) wyników organizacji w zakresie bezpieczeństwa dotyczących:
    - (i.) osiągnięcia jej celów w zakresie bezpieczeństwa;
    - (ii.) wyników jej działań w zakresie monitorowania, w tym ustaleń z audytów wewnętrznych, oraz wewnętrznych dochodzeń prowadzonych w następstwie wypadków lub incydentów oraz statusu odpowiednich działań;
    - (iii.) odpowiednich wyników działań w zakresie nadzoru prowadzonych przez krajowy organ ds. bezpieczeństwa;
  - (d) zaleceń dotyczących doskonalenia.
- 6.3.2. Na podstawie wyników dokonanego przez siebie przeglądu dokonywanego przez kierownictwo, kadra kierownicza wyższego szczebla musi przyjąć ogólną odpowiedzialność za planowanie i wdrażanie niezbędnych zmian w systemie zarządzania bezpieczeństwem.

### 6.3.2 Cel

Silne przywództwo kierownictwa w zakresie bezpieczeństwa ma zasadnicze znaczenie dla sprawnego i skutecznego funkcjonowania systemu zarządzania bezpieczeństwem organizacji, jak również na jej stały rozwój na przestrzeni czasu. Organizacja powinna wykazać, że kierownictwo aktywnie angażuje się w dokonywanie przeglądu w zakresie skuteczności systemu zarządzania bezpieczeństwem i w jego rozwój na przyszłość.

### ***Jak uwzględnić czynniki ludzkie i organizacyjne oraz kulturę bezpieczeństwa?***

Przegląd dokonywany przez kierownictwo jest powiązany ze wszystkimi procesami i procedurami systemu zarządzania bezpieczeństwem, może wówczas uwzględniać czynniki ludzkie i organizacyjne w celu ich doskonalenia.

### 6.3.3 Dowody

- *Procesy dotyczące posiedzeń kierownictwa dotyczących przeglądu systemu zarządzania bezpieczeństwem i postępu związanego z wewnętrznymi zaleceniami z audytów i przeglądów [6.3.1 lit. a)–d)];*
- *rejstry dotyczące sposobu, w jaki organizacja działa zgodnie ze swoimi celami w zakresie bezpieczeństwa [6.3.1 lit. c) ppkt (i)];*

- dowody na to, że w systemie zarządzania bezpieczeństwem wzięto pod uwagę zalecenia odnośnych krajowych organów ds. bezpieczeństwa [6.3.1 lit. c), ppkt (iii)];
- organizacja może wykazać, że posiada procesy do określania i ustalania celów spójnych z rodzajem, zakresem oraz istotnym ryzykiem, regularnie ocenia działalność w odniesieniu do celów, zgodność z procedurami i wykorzystuje dane dotyczące bezpieczeństwa do monitorowania, przeglądu i wdrażania zmian do ustaleń operacyjnych (6.3.1);
- dowody na to, że kadra kierownicza odgrywa czynną rolę w planowaniu i wdrażaniu potrzebnych zmian w systemie zarządzania bezpieczeństwem (6.3.2).
  - istnieją procesy i narzędzia służące do systematycznego zgłaszania i analizowania przyczyn oraz do określania skutecznych środków kontroli dla wszystkich zidentyfikowanych zagrożeń, błędów, wypadków, których uniknięto, wad i incydentów z uwzględnieniem kategoryzacji i analizowania tego, co jest zgłaszane z perspektywy czynników ludzkich i organizacyjnych;
  - w procesie badania wypadków wykorzystuje się wiedzę fachową o czynnikach ludzkich i organizacyjnych;
  - istnieją systematyczne procesy przekazywania doświadczeń z zakresu czynników ludzkich i organizacyjnych dotyczących szkoleń i projektowania;
  - wnioski wyciągnięte z dochodzeń w sprawie wypadków i incydentów są przekazywane pracownikom organizacji oraz są wykorzystywane w szkoleniach, projektowaniu i innych obszarach w celu zmniejszenia prawdopodobieństwa ponownego wystąpienia;
  - wyniki dochodzeń powypadkowych są omawiane na spotkaniach kierownictwa i są uważane za ważne narzędzie do nauki i doskonalenia;
- istnieje proces zapewnienia podczas przeprowadzania dochodzenia w sprawie wypadku.

#### 6.3.4 Przykłady dowodów

Procedura, która obejmuje przegląd i postęp związany z wewnętrznymi zaleceniami z audytów i przeglądów przeprowadzonych przez kadre kierowniczą wyższego szczebla, wraz z protokołami z wybranych posiedzeń.

Dziennik istotnych kwestii przedstawiający wydane zalecenia i postęp związany z naprawą wad zlokalizowanych przez kierownictwo.

Procedura dotycząca przeglądu dokonywanego przez kierownictwo w związku z wynikami wewnętrznego dochodzenia w sprawie wypadku i odnośnymi wynikami nadzoru krajowego organu ds. bezpieczeństwa.

Dostarczane są informacje o tym, które wskaźniki są monitorowane przez kadre kierowniczą wyższego szczebla oraz z jaką częstotliwością.

Przykłady dowodów, o których mowa powyżej, powinny wykazać, w jaki sposób czynniki ludzkie i organizacyjne są zintegrowane z przeglądem dokonywanym przez kierownictwo.

#### 6.3.5 Kwestie związane z nadzorem

Podczas przeprowadzania nadzoru należy zauważyć, czy proces zapewniający, że kadra kierownicza ocenia skuteczność systemu zarządzania bezpieczeństwem, powoduje rzeczywistą zmianę na poziomie operacyjnym.

Kierownictwo jest świadome zmieniających się wewnętrznych i zewnętrznych okoliczności. Czy kadra kierownicza przeprowadza na przykład prognozowanie lub wykorzystuje inne techniki, takie jak analizę PESTLE (analizę czynników politycznych, ekonomicznych, społecznych i technologicznych, środowiskowych i prawnych), aby poinformować o rozwoju swojego systemu zarządzania bezpieczeństwem?

Połączenie/powiązanie między wynikami przeglądu dokonywanego przez kierownictwo, a tym, w jaki sposób stanowią one wkład do rocznego sprawozdania z bezpieczeństwa.

Usprawnianie funkcjonowania  
systemu kolejowego  
na rzecz społeczeństwa.

## 7 Doskonalenie

### 7.1 Wyciąganie wniosków z wypadków i incydentów

#### 7.1.1 Wymóg regulacyjny

|  |
|--|
| <p>7.1. Wyciąganie wniosków z wypadków i incydentów</p> <p>7.1.1. Wypadki i incydenty związane z działalnością kolejową organizacji muszą być:</p> <ul style="list-style-type: none"><li>(a) zgłaszane, rejestrowane, badane i analizowane w celu określenia ich przyczyn;</li><li>(b) w stosownych przypadkach zgłaszane organom krajowym.</li></ul> <p>7.1.2. Organizacja musi zapewnić, by:</p> <ul style="list-style-type: none"><li>(a) zalecenia krajowego organu ds. bezpieczeństwa, krajowego organu dochodzeniowego oraz zalecenia wynikające z dochodzeń branżowych lub wewnętrznych były oceniane i, w stosownych przypadkach, wdrażane lub by zlecano ich wdrożenie;</li><li>(b) analizowane i uwzględniane były stosowne sprawozdania lub informacje pochodzące od innych zainteresowanych stron, takich jak przedsiębiorstwa kolejowe, zarządcy infrastruktury, podmioty odpowiedzialne za utrzymanie i dysponenci pojazdów kolejowych.</li></ul> <p>7.1.3. Organizacja musi korzystać z informacji odnoszących się do dochodzeń na potrzeby przeglądu oceny ryzyka (zob. pkt 3.1.1 Ocena ryzyka), wyciągania wniosków w celu poprawy bezpieczeństwa oraz, w stosownych przypadkach, zastosowania środków naprawczych lub doskonalących (zob. pkt 5.4 Zarządzanie zmianą).</p> |
|--|

#### 7.1.2 Cel

Organizacja powinna wykazać, że przeprowadza dochodzenia w sprawie wypadków i incydentów, aby wyciągać wnioski i doskonalić kontrole ryzyka, że zajmujący się tym personel jest kompetentny do przeprowadzania dochodzenia w sprawie dotyczącej m.in. kwestii związanych z czynnikami ludzkimi i organizacyjnymi, że zgłasza się wypadki do odnośnych organów, a kierownictwo wydaje zalecenia, sporządza sprawozdania i uwzględnia je w swoich działaniach.

Ponadto organizacja stosuje „uczenie się za pomocą podwójnej pętli”: proces uczenia się skupia się nie tylko na rzeczywistym przebiegu wydarzeń, ale także na zdolności organizacji do usprawniania swoich działań, poprzez nacisk na te elementy, które albo wspierają albo hamują przekazywanie wiedzy i informacji w obrębie organizacji.

#### 7.1.3 Noty wyjaśniające

Terminy „wypadki, których uniknięto” oraz „inne niebezpieczne zdarzenia” są zawarte w definicji „incydentu” zgodnie z [dyrektywą \(UE\) 2016/798](#). Niemniej równie istotne znaczenie ma przeprowadzanie dochodzeń w sprawie wypadków, których uniknięto, i innych niebezpiecznych zdarzeń, aby proaktywnie zarządzać bezpieczeństwem.

W ramach wyciągania wniosków z wypadków i incydentów należy wspierać wymianę informacji z innymi zainteresowanymi stronami (zarządcą infrastruktury, innymi przedsiębiorstwami kolejowymi, podmiotami odpowiedzialnymi za utrzymanie – w celu rozwinięcia współpracy i wspierania ogólnej poprawy skuteczności systemu zarządzania bezpieczeństwem).

Osoby przeprowadzające dochodzenia, które wymagają spojrzenia pod kątem czynników ludzkich i organizacyjnych, powinny być albo wyszkolone albo powinny mieć dostęp do odpowiedniej wiedzy fachowej, aby zbadać daną sprawę.

### ***Jak uwzględnić się czynniki ludzkie i organizacyjne oraz kulturę bezpieczeństwa?***

Celem analizy wypadków/incydentów nie jest znalezienie osoby, którą można obarczyć winą, lub działu, który jest „bardziej odpowiedzialny niż inny”, ale raczej zrozumienie i poprawienie słabych stron organizacji, które umożliwiły wystąpienie tych zdarzeń. Najważniejszym wyzwaniem podczas analizowania zdarzeń jest zapobieganie również zdarzeniom „sąsiadującym”. Jeśli zakończy się analizę na zidentyfikowaniu bezpośrednich przyczyn, możliwe będzie jedynie uniknięcie kolejnego podobnego zdarzenia. Jeśli natomiast analiza umożliwi zidentyfikowanie „podstawowych przyczyn” technicznych i organizacyjnych, działania doskonalące pozwolą zapobiec innemu rodzajowi wypadku, którym kierują takie same mechanizmy. Jeśli, na przykład, analiza w wyraźny sposób wykaże, że nie zaktualizowano procedury, i że działania naprawcze mają na celu jedynie poprawę tej procedury, efekt będzie ograniczony. Jeżeli analiza jest głębsza i w jej ramach rozpoznaje się słabe strony w procesie aktualizacji procedur, działania doskonalące mogą wywołać dużo bardziej pozytywny efekt.

Przedsiębiorstwo może skorzystać ze struktury sprawozdań określonej w art. 4 [rozporządzenia \(UE\) 2020/572](#) dotyczącego struktury sprawozdań stosowanej na potrzeby sprawozdań z dochodzeń w sprawie wypadków i incydentów kolejowych, aby określić elementy dotyczące czynników ludzkich i organizacyjnych, które należy zbadać i uwzględnić w swoich sprawozdaniach. Uwaga: jest to jednak tylko jeden z modeli odniesienia, który istnieje i może być używany.

Zachęca się do zgłaszania sytuacji niebezpiecznych i incydentów o „wysokim potencjale” oraz się takie zgłaszanie ułatwia. Istnieją mechanizmy, które zapewniają anonimowość zgłoszeń, jeżeli zachodzi taka potrzeba. Jeżeli zgłoszenia są imienne, pracownicy i zespoły, którzy te zgłoszenia wystali pomagają w zbadaniu sprawy i ustaleniu rozwiązań w krótkiej perspektywie. Organizowane są dyskusje w zespołach, a informacje na temat podjętych działań są przekazywane do właściwych pracowników oraz do innych części organizacji, w zależności od potrzeb.

#### ***7.1.4 Dowody***

- *Informacje dotyczące procesu zgłaszania wypadków/incydentów wraz ze sposobem rozpoznawania i analizowania przyczyn źródłowych, w tym dotyczące zgłaszania wewnątrz organizacji, innym właściwym organom i innym stronom; (7.1.1)*
- *informacje dotyczące metody, którą organizacja wykorzystuje w odniesieniu do dochodzeń uwzględniających kwestie dotyczące czynników ludzkich i organizacyjnych w celu dokonania przeglądu analizy ryzyka i procesu oceny w następstwie zdarzenia; (7.1.3)*
- *dowody na to, że przeprowadzono działania w kwestii zaleceń otrzymanych od właściwych organów, zaleceń ze sprawozdań z wypadków i incydentów oraz wszelkich rozpoznanych niezbędnych zmian; [7.1.2 lit. a), b)]*
- *dokonanie przeglądu przeszłych incydentów w celu wskazania istotnych czynników odnoszących się do bieżącego incydentu lub incydentów. Istnieją dowody na to, że ma miejsce szerokie organizacyjne uczenie się w oparciu o incydenty i doświadczenie, na płaszczyźnie krajowej i międzynarodowej; (7.1.3)*

- *istnieje metodologia prowadzenia badań w oparciu o wiedzę o czynnikach ludzkich i organizacyjnych oraz najnowocześniejsze metody;*
- *istnieje program szkoleniowy dla osób prowadzących dochodzenia w sprawie wypadków i incydentów, w ramach którego stosuje się perspektywę zagadnienia czynników ludzkich i organizacyjnych;*
- *promuje się „kulturę sprawiedliwego traktowania” („just culture”), poprzez rozpoznawanie i wspieranie pozytywnych inicjatyw związanych z bezpieczeństwem (zgłaszanie incydentów, angażowanie pracowników w przeprowadzanie analiz i w proces ciągłych usprawnień, wspieranie współpracowników itp.). Wspomniana „kultura sprawiedliwego traktowania” powinna przyczynić się do wyeliminowania strachu przed obwinianiem, poprzez określenie powszechnie akceptowanych granic między tym co jest akceptowane, a co nie jest. Akceptuje się, że każdy może popełnić błąd.*

#### 7.1.5 Przykłady dowodów

Procedura przeprowadzania dochodzeń w sprawie incydentów opisuje metody dochodzeniowe i uwzględnia odniesienia do wymogów związanych z zarządzaniem kompetencjami, które obowiązują osoby przeprowadzające dochodzenia w sprawie wypadków i incydentów.

Próbka sprawozdań z wypadków i incydentów różnych rodzajów, która wskazuje, że dochodzenia były przeprowadzane przez kompetentną osobę, ustalenia opierały się na dowodach oraz podjęto działania w oparciu o zalecenia.

Kopia procedury/procesu, dzięki któremu śledzi się środki naprawcze/łagodzące, które wskazano w następstwie wypadku/incydu.

Informacje zamieszczone w systemie Informacji o Alertach Bezpieczeństwa SAIT powinny być dostępne na bieżąco. Mają one na celu wspomagać inne organizacje w sprawach dotyczących poszczególnych zasobów.

Dostępni są przeszkoleni pracownicy badający przyczyny wypadków i incydentów.

Uwzględnienie czynników ludzkich i organizacyjnych oraz poprawa kultury bezpieczeństwa będą miały pozytywny wpływ na spełnienie odpowiedniego wymogu systemu zarządzania bezpieczeństwem, a dowody na to można znaleźć w następujących źródłach:

Wymogi dotyczące kompetencji personelu prowadzącego dochodzenia są włączone do systemu zarządzania kompetencjami przedsiębiorstwa. Istnieje program szkoleniowy dla osób prowadzących dochodzenia w sprawie wypadków i incydentów, obejmujący sposób systematycznego uwzględniania czynników ludzkich i organizacyjnych.

Sprawozdania zawierające dogłębną analizę zdarzeń, która prowadzi do opracowania spójnych planów działania na każdym poziomie systemu zarządzania bezpieczeństwem, sprzyjając gotowości do wyciągania wniosków z incydentów poprzez zmianę zachowań w całym przedsiębiorstwie. Protokoły ze spotkań i wymiana komunikatów pokazują, że gdy incydenty obejmują strony zewnętrzne, istnieją dowody na to, że wyniki analizy i działania są ogólnodostępne ogółowi społeczeństwa.

Kadra kierownicza uznaje, że incydenty i wypadki są spowodowane wieloma czynnikami, z których część wynika z decyzji kadry kierowniczej, a protokoły posiedzeń rady pokazują, że rezultaty dochodzeń w sprawie wypadków/incydentów i powiązane z nimi zalecenia (tj. działania naprawcze lub usprawniające) są zgłaszane do kadry zarządzającej – oraz wkład, jaki mają do przeglądu systemu zarządzania bezpieczeństwem (**zob. również 6.3**).

W dochodzeniach w sprawie incydentów i wypadków stosuje się podejście oparte na czynnikach ludzkich i organizacyjnych, a także uwzględnia się je w strategiach dotyczących czynników ludzkich i organizacyjnych oraz kultury bezpieczeństwa, a także we wszystkich powiązanych procesach (ocena ryzyka, ocena wyników, ciągłe doskonalenie...).

Programy szkoleń wstępnych i ustawicznych dla pracowników pokazujące, że działania wynikające ze zdobytych doświadczeń są zintegrowane, ze szczególnym uwzględnieniem ryzyka związanego z czynnikami ludzkimi i organizacyjnymi oraz sposobów jego ograniczania.

W dochodzeniach przyjmuje się perspektywę systematyczną, to znaczy analizuje się nie tylko same czynniki ludzkie, technologiczne i organizacyjne, ale także kładzie się nacisk na interakcje między tymi czynnikami. Na przykład, jeżeli maszynista wziął udział w incydencie przejechania obok sygnału w sytuacji niebezpiecznej (SPAD), czynniki, które należy wziąć pod uwagę w dochodzeniu uwzględniają istotne kwestie np.: zmęczenie, przetładowanie sensoryczne, kompetencje itp. (czynniki ludzkie); wpływ technologii na skuteczność, takie jak interfejs człowiek-system, rozkład, rozmieszczenie sygnałów (czynniki technologiczne); wpływ organizacji na funkcjonowanie, np. szkolenia, system zarządzania bezpieczeństwem, priorytety organizacji (czynniki organizacyjne); a także interakcje między tymi trzema obszarami, na przykład wpływ kwestii związanych z zamawianiem na projektowanie lub zarządzanie zmianą po wprowadzeniu nowego projektu.

Analizę niebezpiecznych zdarzeń przeprowadza się w sposób przekrojowy, wykorzystując szeroki zestaw umiejętności i biorąc pod uwagę punkty widzenia wszystkich zainteresowanych stron (w tym, w stosownych przypadkach, stron zewnętrznych).

Polityka oparta na zasadzie „just culture” i istniejące narzędzia sprawozdawcze sprzyjające kulturze sprawozdawczości i postawie krytycznej wśród pracowników. Wszystkie rutynowe i nietypowe odchylenia zgłaszane przez personel są analizowane i prowadzą do wdrożenia działań usprawniających tam, gdzie jest to konieczne. Systematycznie prowadzona jest komunikacja z zainteresowanym personelem na temat podjętych działań.

#### 7.1.6 Odniesienia i normy

- [Strona internetowa ERA poświęcona kulturze bezpieczeństwa](#)
- [Strona internetowa ERA poświęcona czynnikom ludzkim i organizacyjnym](#)
- [Rozporządzenie wykonawcze Komisji \(UE\) 2020/572 z dnia 24 kwietnia 2020 r. dotyczące struktury sprawozdań stosowanej na potrzeby sprawozdań z dochodzeń w sprawie wypadków i incydentów kolejowych](#)
- MAEA (2002) - *Safety culture in nuclear installations: Guidance for use in the enhancement of safety culture (Kultura bezpieczeństwa w instalacjach jądrowych: wytyczne na temat ulepszania kultury bezpieczeństwa)*. MAEA TECDOC-1529. Międzynarodowa Agencja Energii Atomowej, Wiedeń (2002).
- Mathis, T.L. i Galloway, S.M. (2013) – *Steps to safety culture excellence (Działania mające na celu udoskonalenie kultury bezpieczeństwa)*.
- Kecklund, L., Lavin, M. i Lindvall, J. (2016) - *Safety culture: A requirement for new business models. Lessons learned from other High-Risk Industries. (Kultura bezpieczeństwa: konieczność dla nowych modeli biznesowych. Doświadczenia z innych branż wysokiego ryzyka.)* Odczyt na Międzynarodowej konferencji na temat ludzkich i organizacyjnych aspektów zapewniania bezpieczeństwa nuklearnego – przegląd 30 lat kultury bezpieczeństwa (*The International Conference on Human and Organisational Aspects of Assuring Nuclear Safety – Exploring 30 Years of Safety Culture*), Wiedeń, od 22 do 26 lutego 2016 r.
- RSSB (2015) - *Safety Culture and behavioural development: Common factors for creating a culture of continuous development (Kultura bezpieczeństwa i zmiany w zachowaniu: Główne czynniki pozwalające na utworzenie kultury ciągłego rozwoju)* ([www.sparkrail.org](http://www.sparkrail.org))



### 7.1.7 *Kwestie związane z nadzorem*

Kompetencje osób prowadzących dochodzenia w sprawie wypadków/incydentów mają kluczowe znaczenie w kwestii wskazywania wartościowych zaleceń i wprowadzania stosownych środków zapobiegawczych. Osoby przeprowadzające działania nadzorcze powinny sprawdzać, czy na poziomie zarządczym nie wystąpiła ingerencja w rezultaty sprawozdań z wypadków i incydentów, która może wpłynąć na jakość sprawozdania i wszelkie dalsze skutki, które mogą na tej podstawie nastąpić.

Rezultaty dochodzenia wewnętrznego doprowadziły do stosowania procesów organizacyjnego uczenia się, których ślad widać w dokumentach, sprawozdaniach lub innych kanałach informacyjnych (tj.: intranet, wewnętrzna gazeta firmowa, itp.)

Kultura organizacyjna odnosząca się do zgłaszania incydentów i sytuacji, w których prawie doszło do incydentu.

## 7.2 Ciągłe doskonalenie

### 7.2.1 Wymóg regulacyjny

|   |
|---|
| <p>7.2.1. Organizacja musi stale zwiększać adekwatność i skuteczność swojego systemu zarządzania bezpieczeństwem, uwzględniając ramy określone w rozporządzeniu (UE) nr 1078/2012, a co najmniej wyniki następujących działań:</p> <ul style="list-style-type: none"><li>(a) monitorowania (zob. pkt 6.1 Monitorowanie);</li><li>(b) audytu wewnętrznego (zob. pkt 6.2 Audyt wewnętrzny);</li><li>(c) przeglądu dokonywanego przez kierownictwo (zob. pkt 6.3 Przegląd dokonywany przez kierownictwo);</li><li>(d) wyciągania wniosków z wypadków i incydentów (zob. pkt 7.1 Wyciąganie wniosków z wypadków i incydentów).</li></ul> <p>7.2.2. W ramach swoich procesów organizacyjnego uczenia się organizacja musi zapewnić środki motywowania pracowników i innych zainteresowanych stron do aktywnego działania na rzecz poprawy bezpieczeństwa.</p> <p>7.2.3. Organizacja określa strategię ciągłego doskonalenia swojej kultury bezpieczeństwa, opartą na wykorzystaniu wiedzy fachowej i uznanych metod w celu zidentyfikowania kwestii behawioralnych mających wpływ na różne części systemu zarządzania bezpieczeństwem oraz wprowadzenia środków w celu uwzględnienia tych kwestii.</p> |
|---|

### 7.2.2 Cel

Ciągłe doskonalenie jest ważnym elementem posiadania skutecznego systemu zarządzania bezpieczeństwem. Wymóg ten ma na celu skłonienie wnioskodawcy do wykazania, że zobowiązuje się do ciągłej poprawy i że jego system zarządzania bezpieczeństwem wspiera ten cel.

Kadra kierownicza wyższego szczebla angażuje się w **kolektywną refleksję**, aby stale poprawiać kulturę bezpieczeństwa organizacji.

Ta kolektywna refleksja jest zawarta w strategii, która ma na celu **cechy kulturowe**, które znacząco wpływają na poziom bezpieczeństwa i które zasługują na lepszą wycenę lub ich zmianę.

### 7.2.3 Noty wyjaśniające

Ciągłe doskonalenie (**7.2.1**) dotyczy przede wszystkim elementów systemu zarządzania bezpieczeństwem, które obejmują ocenę i prowadzą do działań w zakresie doskonalenia, ale nie elementów podlegających już doskonaleniu, gdyż takie elementy objęte są już zakresem działań w zakresie monitorowania.

#### **Jak uwzględnić czynniki ludzkie i organizacyjne oraz kulturę bezpieczeństwa?**

Organizacyjne uczenie się (**7.2.2**) oznacza proces doskonalenia działań dzięki lepszej wiedzy i większemu zrozumieniu.

W tym przypadku definicję kultury bezpieczeństwa (**7.2.3**) podano w pkt 2.1.1 lit. j). Pozytywna kultura bezpieczeństwa motywuje organizacje i osoby fizyczne do dążenia do poprawy bezpieczeństwa i skuteczności działania oraz umożliwia im to. Kultura bezpieczeństwa powoduje wzrost poziomu zadowolenia z pracy i zachowywania miejsc pracy oraz jest korzystna pod względem kosztów. Ponadto może przyczyniać się do sprostania oczekiwaniom regulacyjnym, jako że organy ds. bezpieczeństwa i organy regulacyjne w coraz

większym stopniu uznają znaczenie kultury bezpieczeństwa dla skutecznego zarządzania bezpieczeństwem. Konkretnie pozytywna kultura bezpieczeństwa może prowadzić do:

- ograniczenia ryzyka operacyjnego poprzez bardziej wszechstronną ocenę ryzyka oraz lepsze zrozumienie ryzyka w pracy;
- zmniejszenia liczby wypadków przy pracy poprzez eliminację zagrożeń, które identyfikuje się dzięki zgłaszaniu zdarzeń potencjalnie wypadkowych;
- ograniczenia niebezpiecznych czynności i warunków dzięki większemu zaangażowaniu pracowników oraz rozwijaniu umiejętności przywódczych;
- obniżenia kosztów związanych z wypadkami przy pracy oraz z niebezpiecznymi działaniami i warunkami;
- poprawy skuteczności działania dzięki poprawie szkoleń dla pracowników, zwiększeniu ich zaangażowania oraz ograniczeniu liczby wypadków przy pracy, niebezpiecznych działań i warunków.
- doskonalszych i bardziej wydajnych systemów zarządzania bezpieczeństwem oraz lepszego dostosowania procedur i reguł do realnych potrzeb.

Strategię uważa się za długoterminową ze względu na podstawowe cechy kultury, które powstają w wyniku codziennych interakcji i są trudne do zmiany. Strategia jest uznana i wspierana przez kadrę kierowniczą wyższego szczebla.

Jest wiele sposobów na poprawę kultury bezpieczeństwa, takich jak:

- opracowanie systemu umożliwiającego dzielenie się obawami. Może to zależeć od dojrzałości organizacji, być anonimowym, ale z rosnącym zaufaniem być otwartym i dostępnym dla wszystkich. Ważne jest, aby informacja zwrotna była integralną częścią systemu w celu zapewnienia, aby pracownicy odczuwali zaangażowanie i przynależność;
- zmiana warunków zamawiania i kontraktu w sposób, który będzie promował dobrą kulturę bezpieczeństwa wśród dostawców. Kultura bezpieczeństwa może stanowić kryterium wyboru dostawców;
- widoczne nagradzanie bezpiecznego postępowania. Nagroda może mieć wiele postaci – od zwiększenia wynagrodzenia w skali roku za pomocą bonusów po cotygodniowe przyznawanie nagród za wyjątkową skuteczność w dziedzinie bezpieczeństwa;
- opracowanie konkretnych celów dla menedżerów w zakresie postawy przywódczej w kwestii bezpieczeństwa, na przykład zachęcając kierownictwo do odgrywania bardziej widocznej roli w dziedzinie ustalania standardów na podstawie przykładów;
- itd.

Wyniki ocen powinny zostać ogłoszone na wszystkich szczeblach organizacji. Należy podjąć na ich podstawie działania w celu wspierania i podtrzymywania pozytywnej kultury bezpieczeństwa, ulepszenia przywództwa w zakresie bezpieczeństwa i promowania w organizacji postawy ciągłego uczenia się.

Identyfikacja i wybór odpowiednich cech kulturowych jest często złożonym zadaniem<sup>1</sup>, które powinno być starannie przeprowadzone.

W rzeczywistości zadanie to powinno angażować pracowników na wszystkich szczeblach w całej organizacji, a często również poza nią (np. wykonawców).

Spostrzeżenia i przekonania personelu mogą być gromadzone za pomocą ankiety, ale taka metoda jest ogólnie uważana za niewystarczającą do ustalenia cech kulturowych, które wpływają na bezpieczeństwo. W miarę możliwości kierując się wynikami ankiety, eksperci powinni przeprowadzić obserwacje, wywiady indywidualne i grupy fokusowe w celu ustalenia dokładniejszej diagnozy.

---

<sup>1</sup> Różnorodność działań i wielkość organizacji to proste przykłady parametrów związanych ze złożonością tego zadania.

Uwaga: grupa fokusowa to niewielka liczba osób (zazwyczaj od 4 do 15) wraz z moderatorem, która pozwala skupić się na konkretnym temacie. Celem grup fokusowych jest dyskusja, a nie udzielanie konkretnych odpowiedzi na pytania formalne, dzięki czemu można pozyskać jakościowe dane. Na podstawie takiej diagnozy plan działania, który ma na celu lepsze docenianie lub przyczynianie się do zmiany cech kulturowych, może być zdefiniowany i wspierany przez kadrę kierowniczą wyższego szczebla. Kadra kierownicza wyższego szczebla monitoruje wdrażanie zidentyfikowanych działań i odpowiednio je zmienia.

W celu zapewnienia zrównoważonego rozwoju strategii co 2–5 lat organizacja powinna dokonać weryfikacji postawionej diagnozy przy użyciu tego samego podejścia. Częstotliwość zależy od wyników wstępnych działań.

W kilku branżach wysokiego ryzyka diagnoza ta jest często przeprowadzana w ramach *oceny kultury bezpieczeństwa*. Ocena kultury bezpieczeństwa może być przeprowadzona niezależnie lub przez samoocenę. Zaletą niezależnej oceny jest to, że organizacja uzyskuje bardziej obiektywny obraz kultury bezpieczeństwa, ale niesie ryzyko, że organizacja może zostać źle zrozumiana lub mieć trudności z zaakceptowaniem wniosków. Zaletą samooceny jest to, że jest przeprowadzana wewnątrznie z personelem organizacji, który ma dogłębną wiedzę na temat organizacji. Wadą jest to, że status i hierarchie mogą kolidować i utrudniać ocenę. Niektóre cechy charakterystyczne oceny kultury bezpieczeństwa to:

- *2/3-tygodniowy proces oceny i etap przygotowawczy;*
- *zaangażowanie interdyscyplinarnego zespołu oceniającego;*
- *gromadzenie danych opiera się na metodach z zakresu nauk społecznych (w tym wywiadach, grupach fokusowych, obserwacjach);*
- *zakres oceny to cała organizacja i jej interfejsy;*
- *oparta o model kultury bezpieczeństwa lub strukturę;*
- *zaangażowanie kadry kierowniczej wyższego szczebla, która uważa tę ocenę za możliwość uczenia się;*
- *wyniki są rozpowszechniane w całej organizacji;*
- *wyniki są rozpatrywane w celu zaprojektowania/zmiany strategii, w celu ciągłego ulepszania wybranych cech kultury bezpieczeństwa.*

Integralną częścią ciągłego doskonalenia systemów zarządzania bezpieczeństwem jest poprawa strategii i procesów w zakresie czynnika ludzkiego i organizacyjnego.

Systematyczne podejście oznacza stopniowy proces rozwiązywania kwestii związanych z kulturą bezpieczeństwa. Przykładowo oznacza to istnienie procesu monitorowania ryzyka, zgłaszania incydentów i wypadków, a także obejmuje to sposób wykorzystywania informacji oraz wnioski wyciągnięte w zakresie ciągłego doskonalenia.

Więcej informacji na temat kultury bezpieczeństwa oraz czynników ludzkich i organizacyjnych można znaleźć odpowiednio w częściach Załącznik 4 i Załącznik 5.

#### 7.2.4 Dowody

- *Informacje dotyczące procesu zestawiania dowodów w celu wykazania ciągłego doskonalenia systemu zarządzania bezpieczeństwem; (7.2.1)*
- *procedury wyszczególniające, w jaki sposób organizacja uwzględnia wyniki monitorowania, audytu wewnętrznego, przeglądu dokonywanego przez kierownictwo oraz wyniki związane z wnioskami z wypadków i incydentów w celu doskonalenia systemu zarządzania bezpieczeństwem; (7.2.1)*
- *informacje na temat sposobu, w jaki organizacja dąży do angażowania pracowników i innych osób w doskonalenie systemu zarządzania bezpieczeństwem; (7.2.2)*
- *wnioskodawca powinien w strategii szczegółowo opisać, w jaki sposób rozwija się kultura bezpieczeństwa, aby ryzyko związane z kulturą bezpieczeństwa zostało odpowiednio uwzględnione*

w odpowiednich procesach systemu zarządzania bezpieczeństwem. Jednocześnie wnioskodawca powinien jasno wskazać, gdzie można znaleźć dalsze informacje dotyczące odpowiednich procedur; **(7.2.3)**

- *kultura bezpieczeństwa jest ciągle oceniana w celu identyfikacji możliwości udoskonalania; **(7.2.3)***
- *do poprawy kultury bezpieczeństwa jest stosowany cykl PDCA, w celu zapewnienia, że podejmowane działania wywierają wpływ. Wyciągnięte wnioski są realizowane i systematycznie oceniane pod kątem wpływu. **(7.2.3)***

### 7.2.5 Przykłady dowodów

Procedura obejmująca monitorowanie, audyt wewnętrzny, przegląd dokonywany przez kierownictwo oraz dochodzenia w sprawie wypadków i incydentów, szczególnie sekcje poświęcone wnioskowi wyciąganym z doświadczenia zyskanego w ramach systemu zarządzania bezpieczeństwem.

Inicjatywa „Close Call” realizowana przez [Network Rail](#), w przypadku której pracowników zachęca się do aktywnego zgłaszania organizacji słabych stron/luk lub sytuacji, w których zachodzi ryzyko dla bezpieczeństwa lub zdrowia.

Uwzględnienie czynników ludzkich i organizacyjnych oraz poprawa kultury bezpieczeństwa będą miały pozytywny wpływ na spełnienie odpowiedniego wymogu systemu zarządzania bezpieczeństwem, a dowody na to można znaleźć w następujących źródłach:

Przykłady protokołów okresowych posiedzeń związku zawodowego/zarządu poświęconych kwestii zdrowia i bezpieczeństwa, na których omówiono sytuacje, które wydają się niepewne/niebezpieczne lub które wymagają dalszego rozważenia.

Wyniki dochodzeń w sprawie wypadków są przedstawiane na spotkaniach kadry kierowniczej i uznaje się je za ważne narzędzie uczenia się i doskonalenia, uwzględniające czynniki ludzkie i organizacyjne w sposób systemowy i systematyczny.

Egzemplarz strategii na rzecz doskonalenia kultury bezpieczeństwa i wyjaśnienie, w jaki sposób jest ona powiązana z różnymi częściami systemu zarządzania bezpieczeństwem.

Strategia zawiera odpowiednie dowody na posiadanie kompetencji zawodowych i, w razie potrzeby, na prowadzenie szkoleń i posiadanie doświadczenia w dziedzinie kultury bezpieczeństwa wśród personelu na potrzeby opracowania i wprowadzenia strategii.

Wymagane szkolenia i kompetencje wiążą się ze zrozumieniem pojęcia kultury bezpieczeństwa oraz sposobów pomiaru i wypracowania ciągłego doskonalenia. Kluczową kwestią jest pojmowanie kultury bezpieczeństwa jako całościowego pojęcia, które ma wpływ na wszystkie części systemu zarządzania bezpieczeństwem i nie może być traktowane jako odrębny element rządzący się własnymi prawami.

Istnieje proces ciągłej oceny środków poprawy bezpieczeństwa. Skutki zastosowania środków poprawy bezpieczeństwa są identyfikowane po wdrożeniu w praktyce, aby można je było poddać ocenie.

Protokoły z przeglądu dokonywanego przez kierownictwo pokazują, że kadra kierownicza uznaje, iż incydenty, wypadki i odchylenia są spowodowane wieloma czynnikami, z których niektóre mają swoje źródło w procedurach i decyzjach kadry kierowniczej.

Protokoły z posiedzeń dotyczących przeglądu dokonywanego przez kierownictwo pokazują, w jaki sposób działania naprawcze wynikające z działań monitorujących, audytów wewnętrznych oraz procesu badania incydentów i wypadków uwzględniają czynniki ludzkie i organizacyjne i są zdefiniowane na każdym poziomie systemu zarządzania bezpieczeństwem i organizacji. Pokazują również, jak wyniki są wykorzystywane do poprawy oceny ryzyka (**zob. 3.1**).

Procedury obejmujące monitorowanie, audyt wewnętrzny, przegląd dokonywany przez kierownictwo oraz badanie wypadków i incydentów są powiązane z procesem zwiększania świadomości (**zob. 4.3**) i systemem zarządzania kompetencjami (**zob. 4.2**).

#### *7.2.6 Kwestie związane z nadzorem*

W ramach nadzoru należy zbadać zaangażowanie ze strony kierownictwa do ciągłego doskonalenia systemu zarządzania bezpieczeństwem, przeprowadzając rozmowy i analizując dokumentację. Czy doskonalenie opiera się na podejściu opartym na analizie ryzyka, tj. związanym z wrażliwymi i krytycznymi kontrolami?

Należy zbadać wykorzystanie przez organizację modeli dojrzałości do badania wyników systemu zarządzania bezpieczeństwem, jeżeli takie modele istnieją.

**Załącznik 1 – Tabele korelacji**

Poniższe tabele zawierają szczegółowe porównanie między wymogami oceny określonymi w załączniku II do poprzednich rozporządzeń (UE) nr 1158/2010 i (UE) nr 1169/2010 a wymogami określonymi w załącznikach I i II do rozporządzenia (UE) 2018/762. Ma to na celu ułatwienie przejście ze stosowania starego systemu certyfikacji bezpieczeństwa określonego w dyrektywie 2004/49/WE na stosowanie nowego systemu wprowadzonego [dyrektywą \(UE\) 2016/798](#).

Podobieństwo do rozporządzenia (UE) 2018/762 nie stanowi dowodu, że przedsiębiorstwa kolejowe lub zarządcy infrastruktury są w stanie spełnić odpowiednie wymogi dotyczące systemu zarządzania bezpieczeństwem zgodnie z art. 9 [dyrektywy \(UE\) 2016/798](#). Poziom szczegółowości wcześniejszych i nowych wymogów dotyczących oceny nadal może być różny, chociaż w pewnym stopniu wymogi te opierają się na wspólnych zasadach. Ponadto nie wszystkie wymogi dotyczące oceny, określone w załącznikach I i II do [rozporządzenia \(UE\) 2018/762](#) mają swoje odpowiedniki w poprzednich rozporządzeniach. W takiej sytuacji przedsiębiorstwa kolejowe i zarządcy infrastruktury muszą wykazać ponadto, że spełniają nowe wymogi dotyczące oceny (lub część z nich).

Wymogi dotyczące systemu zarządzania bezpieczeństwem określone w [rozporządzeniu \(UE\) 2018/762](#), które nie posiadają żadnych odpowiedników wśród wymogów określonych w rozporządzeniu (UE) nr 1158/2010 lub rozporządzeniu (UE) nr 1169/2010, uznaje się za nowe wymogi, w odniesieniu do których wnioskodawca musi przedstawić dodatkowe dowody, aby wykazać przestrzeganie takich wymogów. W większości przypadków nie jest możliwe idealne dopasowanie kryteriów wcześniejszego rozporządzenia CSM i wymogów nowego rozporządzenia CSM. W takich sytuacjach podstawą porównania jest cel wymogów. Ponadto wymogi sformułowane w [rozporządzeniu \(UE\) 2018/762](#) mogą być bardziej jednoznaczne, a jednocześnie może im przyświecać ten sam cel. W takim przypadku wymogów określonych w tym rozporządzeniu nie uznaje się za nowe, a różne strony mogą je stosować po to, aby lepiej zrozumieć, jakich dowodów oczekuje się od wnioskodawcy.

Istnieje również podobieństwo do ISO High Level Structure (HLS)<sup>2</sup>, co działa na korzyść przedsiębiorstw kolejowych i zarządców infrastruktury chcących opracować zintegrowany system zarządzania. Podobnie posiadanie systemu zarządzania certyfikowanego na podstawie co najmniej jednej normy ISO dotyczącej systemu zarządzania (np. ISO 9001, ISO 14001 lub ISO 45001) nie stanowi dowodu, że przedsiębiorstwa kolejowe lub zarządcy infrastruktury są w stanie spełnić odpowiednie wymogi dotyczące systemu zarządzania bezpieczeństwem zgodnie z art. 9 [dyrektywy \(UE\) 2016/798](#).

*Tabela 1: Szczegółowe porównanie – Kryteria/wymogi oceny wspólne dla przedsiębiorstw kolejowych i zarządców infrastruktury*

| <i>ID kryterium z rozporządzeń (UE) nr 1158/2010 i (UE) nr 1169/2010</i> | <i>Rozporządzenie (UE) 2018/762 ID wymogu</i> | <i>ISO HLS Pkt</i> | <i>Uwagi</i> |
|--|---|--------------------|--------------|
| A.1  | 3.1.1.1                                       | 6.1                |              |
| A.2  | 3.1.1.1                                       | 6.1                |              |
| A.3  | 6.1.1   | 9.1                |              |
| A.4  | 3.1.1.1 e)                                    | n.d.               |              |

<sup>2</sup> Dyrektywy ISO/IEC, część 1, skonsolidowany suplement z 2016 r., załącznik SL, dodatek 2.

| <i>ID kryterium z rozporządzeń (UE) nr 1158/2010 i (UE) nr 1169/2010</i> | <i>Rozporządzenie (UE) 2018/762 ID wymogu</i> | <i>ISO HLS Pkt</i> | <i>Uwagi</i>   |
|--|---|--------------------|--|
| A.5  | 4.4<br>4.5.1.1                                | 7.4                |  |
| A.6  | 6.1.1<br>5.4.1                                | 9.1<br>8.1         |  |
| B.1  | 5.2.4   | n.d.               | Utrzymanie stanowi element cyklu życia aktywów.  |
| B.2  | 5.2.4   | n.d.               | Utrzymanie stanowi element cyklu życia aktywów.  |
| B.3  | 2.3.1<br>4.2.1                                | 5.3<br>7.2         | Określenie i podział obowiązków w zakresie utrzymania w dużej mierze ujęto w pkt 2.3.1<br>Określenie kompetencji wymaganych w zakresie utrzymania w dużej mierze ujęto w pkt 4.2.1   |
| B.4  | 6.1.1<br>5.2.5                                | 9.1<br>7.4         | Gromadzenie danych (awarie, usterki) i analiza stanowią element procesu monitorowania.<br>Wymiana danych między osobami odpowiedzialnymi za codzienne funkcjonowanie a osobami odpowiedzialnymi za utrzymanie stanowi element procesu informacyjno-komunikacyjnego stosowanego w zarządzaniu aktywami. |
| B.5  | 6.1.1   | n.d.               | Art. 4 ust. 2 rozporządzenia w sprawie wspólnej metody oceny bezpieczeństwa w odniesieniu do monitorowania.  |
| B.6  | 6.1.1   | 9.1                | Ocena funkcjonowania i wyników utrzymania stanowi element procesu monitorowania utrzymania.  |
| C.1  | 5.3.2 a)<br>5.3.3 a)                          | 8.1                |  |
| C.2  | 5.3.3 a)                                      | 8.1                |  |
| C.3  | 5.3.2 b)                                      | n.d.               |  |
| C.4  | 5.2.5 b)<br>5.3.2 c)                          | n.d.               |  |
| C.5  | 5.3.2 c)<br>5.3.3 a)                          | n.d.               |  |
| D.1  | 3.1.1.1 a)                                    | n.d.               |  |
| D.2  | 3.1.1.1 c)                                    | n.d.               |  |
| D.3  | 6.1.1   | n.d.               |  |
| E.1  | 1.1.1 a)<br>1.1.1 b)                          | 4.1                |  |
| E.2  | 4.5.1.1 a)                                    | 4.4                |  |
| E.3  | 4.5.1.1 c)                                    | 7.5.1              |  |



| <i>ID kryterium z rozporządzeń (UE) nr 1158/2010 i (UE) nr 1169/2010</i> | <i>Rozporządzenie (UE) 2018/762 ID wymogu</i>  | <i>ISO HLS Pkt</i> | <i>Uwagi</i>   |
|--|--|--------------------|--|
| E.4  | 4.5.1.1 a)<br>4.5.1.1 b)                       | 7.5.1              |  |
| F.1  | 4.5.1.1 a)                                     | 4.4                |  |
| F.2  | 2.3<br>4.5.1.1 a)                              | 5.3<br>4.4         |  |
| F.3  | 2.3.1<br>2.3.4                                 | n.d.               |  |
| F.4  | 4.5.1.1 a)<br>4.2.1<br>2.3.1<br>2.3.2<br>2.3.3 | 4.4<br>5.3         | Określenie zadań związanych z bezpieczeństwem stanowi element opisu systemu zarządzania bezpieczeństwem i obejmuje podział obowiązków. Obowiązki są określane dla każdej stosownej funkcji w systemie zarządzania bezpieczeństwem.   |
| G.1  | 4.5.1.1 a)<br>2.3.1                            | 4.4<br>5.3         | Określenie zadań związanych z bezpieczeństwem stanowi element opisu systemu zarządzania bezpieczeństwem i obejmuje podział obowiązków. Obowiązki są określane dla każdej stosownej funkcji w systemie zarządzania bezpieczeństwem.   |
| G.2  | 6.1.1<br>6.2.1                                 | 9.1<br>9.2         | Audyt wewnętrzny ma na celu sprawdzenie, czy organizacja przestrzega mających zastosowanie wymogów.  |
| G.3  | 2.1.1 d) (i)<br>2.3.2                          | n.d.               |  |
| G.4  | 2.3.1  | 5.3                |  |
| G.5  | 4.1.1  | 7.1                | Należy pamiętać, że istnieje link do Kryterium w 1158/2010 N2 (d)  |
| H.1  | 2.4.1  | n.d.               |  |
| H.2  | (usunięto)                                     | n.d.               | Pracownicy wykonujący zadania związane z bezpieczeństwem powinni uczestniczyć w opracowywaniu, utrzymaniu i doskonaleniu systemu zarządzania bezpieczeństwem. W gestii organizacji pozostawia się wdrożenie wymogu 2.4.1 w sposób umożliwiający identyfikowalność zgodności z nim. |
| I  | 7.2.1  | 10.1<br>10.2       |  |
| J  | 2.2.1  | 5.2                |  |
| K.1  | 3.2.1<br>3.2.2 d)                              | 6.2                |  |
| K.2  | 3.2.2 a)                                       | 6.2                | Cele w zakresie bezpieczeństwa powinny być spójne ze strategią w zakresie bezpieczeństwa, która powinna być odpowiednia do rodzaju i zakresu działalności kolejowej.   |

| <i>ID kryterium z rozporządzeń (UE) nr 1158/2010 i (UE) nr 1169/2010</i> | <i>Rozporządzenie (UE) 2018/762 ID wymogu</i>  | <i>ISO HLS Pkt</i> | <i>Uwagi</i>   |
|--|--|--------------------|--|
| K.3  | 3.2.4  | 6.2                | Cele w zakresie bezpieczeństwa nie ograniczają wspólnych wymagań bezpieczeństwa ustanowionych na szczeblu państwa członkowskiego.  |
| K.4  | 6.1.1<br>5.4                                   | 9.1<br>8.1         |  |
| K.5  | 3.2.4<br>(dostosowany)                         | 9.1                | Odniesienie do strategii i planów monitorowania zgodnych ze wspólnymi metodami oceny bezpieczeństwa w odniesieniu do monitorowania.  |
| L.1  | 6.1.1<br>5.4                                   | 9.1<br>8.1         |  |
| L.2  | 4.2<br>4.4<br>4.5<br>5.2.2 a)                  | n.d.               | Korzystaniem z umiejętności kompetentnych pracowników, procedur, szczególnych dokumentów i taboru kolejowego zarządzają odpowiednio system zarządzania kompetencjami, system zarządzania informowaniem i komunikowaniem, system zarządzania dokumentacją i system zarządzania składnikami aktywów. |
| L.3  | 1.1.1 e)<br>6.1.1<br>6.1.2                     | 4.3<br>9.2         | Zgodność z mającymi zastosowanie wymogami jest w dużej mierze związana z pkt 3.1.2.2 (nie jest specyficzna dla utrzymania).<br>Monitorowanie zapewnia poprawne stosowanie procedur.<br>Przeprowadzanie audytów wewnętrznych zapewnia zgodność procedur z mającymi zastosowanie wymogami.           |
| M.1  | 3.1.2.1<br>5.4.1                               | 6.1<br>8.1         | Zgodnie z ISO w pierwszej kolejności następuje planowanie zmiany, w tym identyfikacja i ocena ryzyka, następnie wdrożenie zmiany.  |
| M.2  | 3.1.2.1  | n.d.               |  |
| M.3  | 5.4.1  | 8.1                |  |
| N.1  | 4.2.1<br>4.2.3                                 | 7.2                |  |
| N.2  | 4.5.1.1 a)<br>2.3.1<br>2.3.2<br>2.3.4<br>6.1.1 | n.d.               |  |
| O.1  | 4.4.1<br>4.4.2<br>4.4.3                        | 7.4                |  |
| O.2  | 4.4.3  | 7.4                |  |

| <i>ID kryterium z rozporządzeń (UE) nr 1158/2010 i (UE) nr 1169/2010</i> | <i>Rozporządzenie (UE) 2018/762 ID wymogu</i> | <i>ISO HLS Pkt</i> | <i>Uwagi</i> |
|--|---|--------------------|--------------|
| O.3  | 4.4.1   | n.d.               |              |
| P.1  | 4.4.3   | n.d.               |              |
| P.2  | 4.5.2<br>4.5.3                                | 7.5.2<br>7.5.3     |              |
| P.3  | 4.5.3   | 7.5.3              |              |
| Q.1  | 7.1.1   | 10.1               |              |
| Q.2  | 7.1.2   | n.d.               |              |
| Q.3  | 7.1.3   | 10.2               |              |
| R.1  | 5.5.1   | n.d.               |              |
| R.2  | 5.5.2   | n.d.               |              |
| R.3  | 5.5.3   | n.d.               |              |
| R.4  | 5.5.4   | n.d.               |              |
| R.5  | 5.5.5   | n.d.               |              |
| R.6  | 5.5.1   | n.d.               |              |
| R.7  | 5.5.6   | n.d.               |              |
| S.1  | 6.2.1   | 9.2                |              |
| S.2  | 6.2.1 a)                                      | 9.2                |              |
| S.3  | 6.2.1 b)                                      | 9.2                |              |
| S.4  | 6.2.1 c)–f)                                   | 9.2                |              |
| S.5  | 6.2.1 g)<br>6.3.1                             | 9.3                |              |
| S.6  | 6.2.1   | 9.2                |              |

W tabeli poniżej przedstawiono szczegółowe porównanie poprzednich kryteriów oceny i nowych wymogów dotyczących systemu zarządzania bezpieczeństwem, które mają zastosowanie wyłącznie do przedsiębiorstw kolejowych.

Tabela 2: Szczegółowe porównanie – Kryteria oceny/wymogi dotyczące przedsiębiorstw kolejowych

| ID kryterium z rozporządzenia (UE) nr 1158/2010 | Rozporządzenie (UE) 2018/762 załącznik I ID wymogu | ISO HLS Pkt | Uwagi |
|---|--|-------------|-------|
| R.8   | 5.5.7  | n.d.        |       |
| R.9   | 5.5.8  | n.d.        |       |

W tabeli poniżej przedstawiono szczegółowe porównanie poprzednich kryteriów oceny i nowych wymogów dotyczących systemu zarządzania bezpieczeństwem, które mają zastosowanie wyłącznie do zarządców infrastruktury.

Tabela 3: Szczegółowe porównanie – Kryteria oceny/wymogi dotyczące zarządców infrastruktury

| ID kryterium z rozporządzenia (UE) nr 1169/2010 | Rozporządzenie (UE) 2018/762 załącznik II ID wymogu | ISO HLS Pkt | Uwagi   |
|---|---|-------------|---|
| R.8   | 5.5.7   | n.d.        |   |
| R.9   | 5.5.8   | n.d.        |   |
| T.1   | 5.2.1   | n.d.        | Bezpieczna konstrukcja i instalacja infrastruktury są częścią cyklu życia aktywów.  |
| T.2   | 3.1.2<br>5.4.1                                      | n.d.        | Identyfikację technicznej zmiany infrastruktury w dużej mierze ujęto w pkt 3.1.2.<br>Zarządzanie techniczną zmianą infrastruktury w dużej mierze ujęto w pkt 5.4.1. |
| T.3   | 3.1.2   | n.d.        | Zgodność z mającymi zastosowanie przepisami dotyczącymi konstrukcji infrastruktury w dużej mierze ujęto w pkt 3.1.2.  |
| U.1   | 5.1.1<br>5.1.3                                      | n.d.        | Zarządzanie bezpieczeństwem infrastruktury w dużej mierze ujęto w pkt 5.1.1.  |
| U.2   | 5.1.1   | n.d.        | Zarządzanie bezpieczeństwem na fizycznych lub operacyjnych granicach infrastruktury w dużej mierze ujęto w pkt 5.1.1.   |
| U.3   | 5.1.3 c)<br>5.5.7                                   | n.d.        | Zarządzanie w normalnych warunkach działalności i w sytuacji awarii w dużej mierze ujęto w pkt 5.1.3 lit. c).   |
| U.4   | 5.1.2<br>5.2.3                                      | n.d.        |   |
| V.1   | 5.2.4<br>6.1.1                                      | n.d.        | Utrzymanie infrastruktury w dużej mierze ujęto w pkt 5.2.4.<br>Audyty i inspekcje (w stosownych przypadkach) są częścią działań w zakresie monitorowania.           |
| V.2   | 5.2.4   | n.d.        | Utrzymanie infrastruktury w dużej mierze ujęto w pkt 5.2.4.   |
| V.3   | 5.2.3   | n.d.        |   |

| <i>ID kryterium z rozporządzenia (UE) nr 1169/2010</i> | <i>Rozporządzenie (UE) 2018/762 załącznik II ID wymogu</i> | <i>ISO HLS Pkt</i> | <i>Uwagi</i>  |
|--|--|--------------------|---|
| W.1  | 5.1.3  | n.d.               |   |
| W.2  | 5.1.1  | n.d.               | Zarządzanie bezpieczeństwem na fizycznych lub operacyjnych granicach systemu sterowania ruchem kolejowym i sygnalizacji w dużej mierze ujęto w pkt 5.1.1. |
| W.3  | 5.1.2<br>5.2.3   | n.d.               |   |

W tabeli poniżej przedstawiono szczegółowe porównanie ISO HLS i nowych wymogów dotyczących systemu zarządzania bezpieczeństwem.

*Tabela 4: Szczegółowe porównanie – ISO High Level Structure*

| <i>ISO HLS Pkt</i> | <i>Rozporządzenie (UE) 2018/762 ID wymogu</i> | <i>Uwagi</i>  |
|--------------------|---|---|
| 4.1                | 1.1.1 a)<br>1.1.1 b)                          |   |
| 4.2                | 1.1.1 c)<br>1.1.1 d)                          |   |
| 4.3                | 1.1.1 e)<br>1.1.1 f)                          |   |
| 4.4                | 4.5.1.1 a)                                    |   |
| 5.1                | 2.1   |   |
| 5.2                | 2.2   |   |
| 5.3                | 2.3   |   |
| 6.1                | 3.1.1<br>3.1.2                                | Wspólną metodę oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka stosuje się, aby określić, czy zmiana jest związana z bezpieczeństwem oraz czy jest znacząca. Ponownie ocenia się wprowadzone przez ISO „wirtualne” rozdzielanie na strategiczny (pkt 6 ISO HLS) i taktyczny (pkt 8 ISO HLS) poziom planowania, uwzględniając ramy regulacyjne UE i, w szczególności, zastosowanie powyższej wspólnej metody oceny bezpieczeństwa (niezależnie od charakteru zmian). |
| 6.2                | 3.2.1<br>3.2.2 a)<br>3.2.2 d)<br>3.2.4        |   |
| 7.1                | 4.1   |   |
| 7.2                | 4.2   |   |

| <i>ISO HLS<br/>Pkt</i> | <i>Rozporządzenie<br/>(UE) 2018/762<br/>ID wymogu</i> | <i>Uwagi</i>  |
|------------------------|---|---|
| 7.3                    | 4.3   |   |
| 7.4                    | 4.4   |   |
| 7.5.1                  | 4.5.1   |   |
| 7.5.2                  | 4.5.2   |   |
| 7.5.3                  | 4.5.3   |   |
| 8.1                    | 5.1<br>5.2<br>5.3<br>5.4<br>5.5                       | Zgodnie z wytycznymi ISO (N360) celem punktu 8 ISO HLS jest określenie wymogów, które należy wdrożyć w ramach działalności organizacji, aby zagwarantować spełnienie wymogów dotyczących systemu zarządzania oraz odniesienie się do najważniejszych zagrożeń i możliwości. Ponadto stwierdza się, że można określić dodatkowe wymogi (dla danej dziedziny) dotyczące planowania operacyjnego i kontroli operacyjnej. Pod tym względem wymogi określone w pkt 5.X są zgodne z podejściem ISO. W szczególności stwierdza się, że wymogi te nie ingerują w działalność gospodarczą przedsiębiorstwa, ale zapewniają wystarczające ramy do kontroli sposobu, w jaki zarządza się kluczowymi kwestiami bezpieczeństwa w ramach procesów gospodarczych przedsiębiorstwa. |
| 9.1                    | 6.1   | Pojęcie „monitorowania” odnosi się do ram monitorowania określonych we wspólnej metodzie oceny bezpieczeństwa w odniesieniu do monitorowania, w związku z czym jest ono rozleglejsze niż pojęcie monitorowania, pomiarów, analizy i oceny określone w pkt 9.1 ISO HLS.  |
| 9.2                    | 6.2   | Audyty wewnętrzne są narzędziami monitorowania w rozumieniu wspólnej metody oceny bezpieczeństwa w odniesieniu do monitorowania. Choć jest to osobny wymóg, ma on na celu osiągnięcie celów monitorowania zgodnie ze wspólną metodą oceny bezpieczeństwa w odniesieniu do monitorowania.  |
| 9.3                    | 6.3   |   |
| 10.1                   | 7.1   |   |
| 10.2                   | 7.2   |   |

## Załącznik 2 – Wzajemna akceptacja zezwoleń, uznań lub certyfikatów produktów lub usług wydawana zgodnie z prawem Unii

Organ wydający jednolity certyfikat bezpieczeństwa lub autoryzację bezpieczeństwa może uznać certyfikaty wydane przez inne organy, takie jak jednostka oceniająca zgodność ISO, aby uniknąć powielania oceny i poniesienia dodatkowych kosztów przez wnioskodawcę. Ostateczna decyzja zawsze należy do organu wydającego.

Zgodnie z art. 3 ust. 12 [rozporządzenia \(UE\) 2018/763](#) do celów oceny wniosków o jednolity certyfikat bezpieczeństwa organ wydający przyjmuje zezwolenia, uznania lub certyfikaty produktów lub usług wydane przez przedsiębiorstwa kolejowe lub ich wykonawców, partnerów lub dostawców, które wydano zgodnie z odnośnym prawem Unii jako dowód spełniania przez przedsiębiorstwa kolejowe odpowiednich wymogów systemu zarządzania bezpieczeństwem dotyczących danego rodzaju produktu lub usługi. Chociaż w prawie Unii nie istnieje przepis równoważny dla oceny wniosków o autoryzację, organy ds. bezpieczeństwa również zachęca się do stosowania tej samej zasady.

W poniższej tabeli zidentyfikowano poszczególne przypadki zaistniałe dotychczas w ramach regulacyjnych Unii i przedstawiono obrazowe przykłady rodzajów produktów lub usług, które mogą zostać objęte każdym przykładem.

*Tabela 5: Zezwolenia, uznania lub certyfikaty produktów lub usług wydawane zgodnie z prawem Unii*

| <i>Przypadek</i>                                   | <i>Rodzaj produktów lub usług</i> | <i>Mające zastosowanie prawo Unii</i>                                | <i>Rozporządzenie (UE) 2018/762 ID wymogu</i> | <i>Uwagi</i>   |
|--|-----------------------------------|--|---|--|
| Certyfikat podmiotu odpowiedzialnego za utrzymanie | Utrzymanie pojazdów               | Art. 14 ust. 4 dyrektywy (UE) 2016/798, rozporządzenie (UE) 2019/779 | 5.2<br>5.3                                    | W przypadkach przewidzianych w art. 14 ust. 4 dyrektywy (UE) 2016/798 certyfikacja podmiotów odpowiedzialnych za utrzymanie zapewnia wystarczający dowód, że przedsiębiorstwa kolejowe i zarządcy infrastruktury – za pośrednictwem swojego systemu zarządzania bezpieczeństwem – są w stanie kontrolować ryzyko związane z utrzymywaniem pojazdów, w tym z korzystaniem z usług wykonawców. |

| <i>Przypadek</i>                 | <i>Rodzaj produktów lub usług</i>      | <i>Mające zastosowanie prawo Unii</i>           | <i>Rozporządzenie (UE) 2018/762 ID wymogu</i> | <i>Uwagi</i>   |
|----------------------------------|--|---|---|--|
| Uznanie                          | Szkolenie maszynistów                  | Dyrektywa 2007/59/WE<br><br>Decyzja 2011/765/UE | 4.2.2   | Właściwe organy powinny uznawać ośrodki szkoleniowe, które prowadzą kursy szkoleniowe dla maszynistów i kandydatów na maszynistów zgodnie z dyrektywą 2007/59/WE. Ośrodki szkoleniowe odgrywają istotną rolę poprzez zapewnianie, aby maszyniści posiadali kompetencje w zakresie przypisywanych im zadań związanych z bezpieczeństwem. W tym zakresie ośrodki szkoleniowe powinny posiadać kompetencje w zakresie prowadzonych przez nie szkoleń, przy czym – w stosownych przypadkach – organ wydający certyfikat bezpieczeństwa i krajowy organ ds. bezpieczeństwa powinny wziąć pod uwagę ich uznanie ze strony właściwego organu podczas dokonywania oceny systemu zarządzania kompetencjami. |
| Licencja i certyfikat maszynisty | Kompetencje i stan zdrowia maszynistów | Dyrektywa 2007/59/WE                            | 4.2.1   | Licencje i certyfikaty wydawane zgodnie z dyrektywą 2007/59/WE stanowią wystarczający dowód odpowiedniego stanu zdrowia i kompetencji maszynistów. Nie przeszkadza to organizacji w wykazaniu, że jej środki określania kompetencji i stanu zdrowia są odpowiednie.  |



| <i>Przypadek</i>                    | <i>Rodzaj produktów lub usług</i>  | <i>Mające zastosowanie prawo Unii</i> | <i>Rozporządzenie (UE) 2018/762 ID wymogu</i> | <i>Uwagi</i>  |
|-------------------------------------|--|---------------------------------------|---|---|
| Jednolity certyfikat bezpieczeństwa | Utrzymanie i inspekcje infrastruktury<br>Manewrowanie<br>Badanie taboru kolejowego | Art. 10 dyrektywy (UE) 2016/798       | 5.3   | Zarządcy infrastruktury mogą zlecać podwykonawstwo utrzymywania lub inspekcji ich infrastruktury przedsiębiorstwom obsługującym szczególne pojazdy na torze.<br>W podobny sposób certyfikat bezpieczeństwa może być wymagany od podmiotów zajmujących się badaniem i manewrowaniem.<br>W opisanych powyżej przypadkach jednolity certyfikat bezpieczeństwa zapewnia wystarczający dowód, że przedsiębiorstwa kolejowe i zarządcy infrastruktury – za pośrednictwem swojego systemu zarządzania bezpieczeństwem – są w stanie kontrolować ryzyko związane z korzystaniem z usług wykonawców i dostawców. |

| <i>Przypadek</i>   | <i>Rodzaj produktów lub usług</i>  | <i>Mające zastosowanie prawo Unii</i> | <i>Rozporządzenie (UE) 2018/762 ID wymogu</i> | <i>Uwagi</i>   |
|--|--|---------------------------------------|---|--|
| Zezwolenie na wprowadzenie do obrotu/<br>dopuszczenie typu pojazdu do eksploatacji | Zezwolenie na wprowadzenie pojazdu do obrotu/<br>dopuszczenie typu pojazdu do eksploatacji | Dyrektywa (UE) 2016/797               | 5.2   | Poprzez swoją konstrukcję, strukturę oraz uwzględnioną w jego ramach weryfikację i zatwierdzenie zezwolenie na wprowadzenie pojazdu do obrotu/dopuszczenie typu pojazdu do eksploatacji zapewnia zgodność z zasadniczymi wymogami całości mającego zastosowanie ustawodawstwa (w tym w zakresie bezpieczeństwa), aby z pojazdu można było bezpiecznie korzystać w sieciach kolejowych, na rzecz których jest on przeznaczony zgodnie z ograniczeniami i warunkami korzystania określonymi w pliku technicznym dotyczącym pojazdu/typu pojazdu. |

W określonych przypadkach posiadanie certyfikatu (bądź jego odpowiednika) wydanego zgodnie z prawem Unii może być niewystarczające do kontrolowania wszystkich obszarów ryzyka dotyczącego produktów dostarczonych przedsiębiorstwom kolejowym i zarządcom infrastruktury lub związanego z usługami, z którym przedsiębiorstwa kolejowe i zarządcy infrastruktury korzystają.

Przykładowo przedsiębiorstwa kolejowe będące w partnerstwie pozostają w pełni odpowiedzialne za bezpieczne funkcjonowanie, a zatem odpowiedzialne za kontrolę ryzyka związanego z ich działalnością, w tym ze świadczonymi usługami utrzymania pojazdów. Korzystanie przez przedsiębiorstwo kolejowe z jednolitego certyfikatu bezpieczeństwa swojego partnera nie jest wystarczającym środkiem kontroli ryzyka związanego ze świadczeniem usług utrzymania, jeżeli nie stoją za nim silne i skuteczne ustalenia umowne zawarte między partnerami. Wspomniane ustalenia umowne muszą być wspólnie opracowane i monitorowane podczas stosowania procedur w ramach systemu zarządzania bezpieczeństwem każdego partnera, przy czym są również częścią każdego systemu zarządzania bezpieczeństwem, w związku z czym podlegają one nadzorowi przez odpowiednie krajowe organy ds. bezpieczeństwa.

Jednolitego certyfikatu bezpieczeństwa można zatem użyć jako środka kontroli ryzyka związanego ze świadczeniem usług utrzymania oraz jako środka zgodności w zakresie spełniania wymogów odnoszących się do kontroli ryzyka związanego z utrzymaniem pojazdów, jeżeli spełnione są następujące trzy warunki:

1. *Między przedsiębiorstwami kolejowymi będącymi partnerami muszą obowiązywać ustalenia umowne, które obejmują aspekty związane z utrzymaniem pojazdów, takie jak:*
  - a) *wymiana informacji opisana w art. 5 [rozporządzenia \(UE\) 2019/779](#);*
  - b) *w stosownych przypadkach wsparcie techniczne, w szczególności w zakresie dotychczasowego systemu kontrolno-decyzyjnego;*

- c) kontrola zdolności zakontraktowanych warsztatów utrzymaniowych do świadczenia usług utrzymania;
  - d) skuteczne monitorowanie pojazdów oraz wymiana informacji uzyskanych w drodze tego monitorowania.
2. Wspomniane ustalenia umowne opracowuje się w oparciu o ocenę ryzyka, przy czym każde przedsiębiorstwo kolejowe powinno je regularnie monitorować pod kątem wspólnej metody oceny bezpieczeństwa w odniesieniu do monitorowania ([rozporządzenie \(UE\) nr 1078/2012](#)). Oba przedsiębiorstwa kolejowe będące partnerami następnie formalnie wymieniają się wynikami tego monitorowania.
3. System zarządzania bezpieczeństwem obu partnerów uwzględnia odpowiednie procesy i procedury, aby spełnić wyżej wymienione warunki 1 i 2.

W innych przypadkach prawo krajowe może wymagać, aby konkretny rodzaj produktu lub usługi posiadał certyfikat krajowy (bądź jego odpowiednik) wydany przez właściwy organ (np. krajowy organ ds. bezpieczeństwa), który mógłby być również wykorzystywany jako dowód spełniania przez przedsiębiorstwa kolejowe lub zarządców infrastruktury odpowiednich wymogów określonych w [rozporządzeniu \(UE\) 2018/762](#). Przykładowo certyfikaty krajowe wydane podmiotom odpowiedzialnym za utrzymanie lub warszatom utrzymaniowym pojazdów innych niż wagony towarowe mogą – podobnie jak certyfikat podmiotu odpowiedzialnego za utrzymanie – stanowić uzasadnione zapewnienie, że pojazdy, za których utrzymanie są one odpowiedzialne, są w stanie umożliwiającym bezpieczną eksploatację.

## Załącznik 3 – Eksploatacja bocznic, ustalenia umowne i partnerstwa

### **Eksploatacja bocznic**

W niniejszym dokumencie „bocznica” oznacza infrastrukturę kolejową połączoną z siecią kolejową, za którą odpowiedzialny jest zarządca infrastruktury (tj. część infrastruktury systemu kolei wchodzącą w zakres stosowania [dyrektywy \(UE\) 2016/798](#)). Bocznice mogą, lecz nie muszą być częścią tej sieci kolejowej, w zależności od transpozycji wyżej wymienionej dyrektywy w każdym państwie członkowskim.

Działania prowadzone na bocznicach, takie jak załadunek wagonów, stanowią działalność przemysłową powiązaną z określonego rodzaju działalnością kolejową, np. zestawianiem, przygotowywaniem i przemieszczaniem zestawów pojazdów, które mogą być pociągami lub które mogą być wykorzystywane w pociągach. Obejmuje to łączenie różnych pojazdów w celu uformowania zestawów pojazdów lub pociągów oraz ich przemieszczanie.

Bocznicami mogą być m.in.:

- *infrastruktura wykorzystywana do postoju pojazdów kolejowych podczas przerw w eksploatacji;*
- *terminale intermodalne;*
- *infrastruktura wykorzystywana do świadczenia usług powiązanych z pojazdami pasażerskimi, takich jak sprzątkanie lub drobne naprawy;*
- *infrastruktura należąca do warsztatów utrzymaniowych pojazdów kolejowych i zarządzana przez te warsztaty;*
- *obszary lub zakłady przemysłowe, gdzie przeprowadza się przemysłowy załadunek/rozładunek wagonów towarowych.*

Działania prowadzone na bocznicach przeprowadza „operator bocznicy”. Operatorem bocznicy może być przedsiębiorstwo kolejowe, zarządca infrastruktury, usługodawca (np. świadczący usługi z zakresu czyszczenia pojazdów pasażerskich), organizacja przemysłowa (np. zakład chemiczny załadowujący/rozładowujący cysterny kolejowe), a nawet podwykonawca wspomnianej organizacji przemysłowej. W pierwszym przypadku organizacja podjęła decyzję biznesową o staniu się przedsiębiorstwem kolejowym lub jest przedsiębiorstwem kolejowym, które oprócz pełnienia swojej bieżącej działalności kolejowej planuje zarządzać bocznicami. W drugim przypadku zarządca infrastruktury jest zarządcą infrastruktury bocznicy lub działa jako przedsiębiorstwo kolejowe na podstawie swojej autoryzacji bezpieczeństwa.

„Operator bocznicy” kontroluje ryzyko związane z bezpieczeństwem i higieną pracy za pośrednictwem systemu zarządzania bezpieczeństwem i zdrowiem, który stosuje zgodnie z prawodawstwem międzynarodowym i krajowym. Jeżeli „operator bocznicy” nie jest przedsiębiorstwem kolejowym, we wspomnianym systemie zarządzania uwzględnia się zobowiązania dotyczące zdrowia i bezpieczeństwa względem pracowników zewnętrznych, w szczególności pracowników przedsiębiorstw kolejowych, np. kiedy maszyniści znajdują się na terenie bocznicy. Równolegle przedsiębiorstwo kolejowe kontroluje ryzyko związane z bezpieczeństwem i higieną pracy za pośrednictwem systemu zarządzania bezpieczeństwem i zdrowiem, który stosuje zgodnie z prawodawstwem międzynarodowym i krajowym.

### **Przypadek 1: Operator bocznicy jest przedsiębiorstwem kolejowym „Y”**

Przedsiębiorstwo kolejowe za pośrednictwem swojego systemu zarządzania bezpieczeństwem kontroluje ryzyko związane ze swoją działalnością kolejową na obszarze infrastruktury bocznicy oraz w obrębie sieci kolejowej na podstawie jego odpowiedzialności zarządcy infrastruktury. Wspomniana kontrola ryzyka obejmuje ryzyko związane z uszkodzeniami pojazdów spowodowanymi wszelkimi działaniami wykonywanymi na bocznicy, w tym również składem, przygotowywaniem i eksploatacją pociągów.

W praktyce czasami trudno jest określić odpowiedzialne przedsiębiorstwo kolejowe. Na przykład pociąg przedsiębiorstwa kolejowego „X” przyjeżdża na bocznice (maszynista i lokomotywa są wynajęci), a przedsiębiorstwo kolejowe „Y”, które obsługuje bocznice, przyjmuje pociąg jako nowy (maszynista i

lokomotywa są wynajęci), a w międzyczasie należy przeprowadzić działania związane z eksploatacją bocznicy. W takim przypadku zastosowanie ma wyżej wymieniona zasada bezpieczeństwa. Istnieje współdzielone ryzyko na płaszczyznach oddziaływań, które należy uwzględnić w systemie zarządzania bezpieczeństwem przedsiębiorstwa kolejowego „Y” (np. uszkodzenia pojazdów spowodowane działaniami prowadzonymi na bocznicy, takimi jak załadunek). Ponadto należy też uwzględnić informacje o pojazdach przekazane przedsiębiorstwu kolejowemu „Y” przez przedsiębiorstwo kolejowe „X”. Obejmuje to zapewnienie, że pojazd jest w stanie umożliwiającym bezpieczną eksploatację w czasie, gdy przedsiębiorstwo kolejowe „X” przekazuje pojazd operatorowi bocznicy oraz gdy przedsiębiorstwo kolejowe „Y” przekazuje pojazd dalej. Odpowiedzialne za eksploatację bocznicy przedsiębiorstwo kolejowe „Y” pozostaje w pełni odpowiedzialne za kontrolę ryzyka nieodłącznego związanego z prowadzoną działalnością mającą na celu utrzymanie.

### **Przypadek 2: Operator bocznicy nie jest przedsiębiorstwem kolejowym**

Można wyróżnić cztery podprzypadki:

- **Podprzypadek 2.1**, jeżeli operator bocznicy jest zarządcą infrastruktury.
- **Podprzypadek 2.2 i 2.3**, jeżeli operator bocznicy niebędący zarządcą infrastruktury prowadzi działalność wyłącznie w obrębie swojej własnej infrastruktury, ale nie na sieci kolejowej, za którą odpowiada zarządca infrastruktury.
- **Podprzypadek 2.4** obejmuje działalność kolejową prowadzoną przez operatora bocznicy niebędącego zarządcą infrastruktury na sieci kolejowej, za którą odpowiada zarządca infrastruktury.

**Podprzypadek 2.1:** Jeżeli działalność na bocznicach dzieli się między przedsiębiorstwo kolejowe (lub przedsiębiorstwa kolejowe) a zarządcę infrastruktury (lub dowolną organizację działającą w jego imieniu), każde przedsiębiorstwo kolejowe należy poinformować o wszystkich wydarzeniach związanych z bezpieczeństwem, które miały miejsce podczas działań przeprowadzonych przez zarządcę infrastruktury na mocy ustaleń umownych. Obejmuje to uszkodzenia, wypadki i incydenty z udziałem pojazdów.

Wspomnianymi ustaleniami umownymi zarządza się odpowiednio za pomocą systemu zarządzania bezpieczeństwem każdego przedsiębiorstwa kolejowego oraz systemu zarządzania bezpieczeństwem zarządcy infrastruktury.

Za pośrednictwem systemu zarządzania bezpieczeństwem przedsiębiorstwo kolejowe kontroluje ryzyko związane ze swoją działalnością w odniesieniu do otrzymanych informacji.

**Podprzypadek 2.2:** Przedsiębiorstwo kolejowe przygotowuje pociąg i jego skład (łączenie, przygotowywanie) w obrębie infrastruktury bocznicy. Przedsiębiorstwo kolejowe musi posiadać informacje na temat wszystkich wydarzeń (związanych z bezpieczeństwem), które miały miejsce podczas działań przeprowadzonych przez operatora bocznicy (np. załadunek bądź czyszczenie) na mocy ustaleń umownych. Obejmuje to uszkodzenia, wypadki i incydenty z udziałem pojazdów.

Wspomnianymi ustaleniami umownymi zarządza się za pomocą systemu zarządzania bezpieczeństwem przedsiębiorstwa kolejowego.

Za pośrednictwem systemu zarządzania bezpieczeństwem przedsiębiorstwo kolejowe kontroluje ryzyko związane ze swoją działalnością następczą w odniesieniu do otrzymanych informacji.

**Podprzypadek 2.3:** Skład pociągu jest w pełni lub częściowo przygotowywany przez operatora bocznicy lub przez organizację działającą w imieniu operatora bocznicy.

Po skompletowaniu składu pociąg przekazuje się jednemu przedsiębiorstwu kolejowemu.

Jak w przypadku podprzypadku 2.2, przedsiębiorstwo kolejowe musi posiadać informacje na temat wszystkich wydarzeń, które miały miejsce podczas działań przeprowadzonych przez operatora bocznicy (np. załadunek bądź czyszczenie) i podczas przygotowywania składu pociągu na mocy ustaleń umownych. Wydarzenia obejmują uszkodzenia, wypadki i incydenty z udziałem pojazdów.

Wspomnianymi ustaleniami umownymi zarządza się za pomocą systemu zarządzania bezpieczeństwem przedsiębiorstwa kolejowego.

Za pośrednictwem systemu zarządzania bezpieczeństwem przedsiębiorstwo kolejowe kontroluje ryzyko związane ze swoją działalnością w odniesieniu do otrzymanych informacji.

**Podprzypadek 2.4:** Ten podprzypadek uzupełnia podprzypadek 2.3. W związku z tym poniżej przedstawiono wyłącznie dodatkowe obowiązki przedsiębiorstwa kolejowego.

Operator boczniczy prowadzi pociągi lub przemieszcza zestawy pojazdów ze swojej infrastruktury kolejowej do sieci kolejowej, za którą odpowiedzialny jest zarządca infrastruktury.

Na przykład:

- *przemieszcza pociąg lub zestawy pojazdów z zajezdni remontowej na perony stacji pasażerskich lub na miejsce postoju znajdujące się przy stacji pasażerskiej;*
- *przemieszcza pociąg lub zestawy pojazdów z zakładu przemysłowego do punktu wymiany (zmiana boczniczy) znajduącego się przy stacji towarowej.*

Operator boczniczy nie jest przedsiębiorstwem kolejowym ani zarządcą infrastruktury, ale wymienione działania prowadzone na sieci zarządcy infrastruktury muszą być objęte jednolitym certyfikatem bezpieczeństwa lub autoryzacją bezpieczeństwa.

Działalność kolejowa prowadzona przez operatora boczniczy na sieci kolejowej, za którą odpowiedzialny jest zarządca infrastruktury, jest objęta jednolitym certyfikatem bezpieczeństwa przedsiębiorstwa kolejowego lub autoryzacją bezpieczeństwa zarządcy infrastruktury. Oznacza to, że przedsiębiorstwo kolejowe lub zarządca infrastruktury musi kontrolować ryzyko związane z działalnością prowadzoną przez operatora boczniczy na podstawie ustaleń zarządzania podwykonawców za pomocą swojego systemu zarządzania bezpieczeństwem.

W każdym przypadku przedsiębiorstwa kolejowe i zarządca infrastruktury muszą w dokładny sposób opisać zakres całej swojej działalności kolejowej i swoich działań, które wiążą je z inną działalnością kolejową, aby skutecznie nadzorować system zarządzania bezpieczeństwem przez krajowe organy ds. bezpieczeństwa. Zdolność przedsiębiorstw kolejowych i zarządców infrastruktury do jasnego i pełnego opisanie prowadzonej przez nich działalności oraz innych działań związanych z eksploatacją kolei ma zasadnicze znaczenie dla zapewnienia skuteczności systemu zarządzania bezpieczeństwem i skuteczności nadzoru krajowego organu ds. bezpieczeństwa.

W ustaleniach umownych we wszystkich wyżej wymienionych podprzypadkach należy ująć m.in.:

- *działania, do których zobowiązują się kontrahenci;*
- *oczekiwaną jakość wyników/usług;*
- *wyznaczone role i obowiązki;*
- *jakimi informacjami, kiedy i w jaki sposób kontrahenci będą się wymieniać. Informacje obejmują sprawozdawczość w zakresie wydarzeń opisanych we wszystkich wyżej wymienionych podprzypadkach oraz szczególne cechy charakterystyczne infrastruktury boczniczy, takie jak ograniczenia prędkości, ograniczenia wagowe i warunki nachylenia;*
- *wymogi w zakresie kompetencji;*
- *wymogi dotyczące zdrowia i bezpieczeństwa (wynikające z oceny ryzyka, wymogów krajowych itp.).*

### **Ustalenia umowne i partnerstwa**

Przedsiębiorstwo kolejowe odpowiada za zapewnienie możliwości bezpiecznej eksploatacji pojazdu poprzez koordynowanie i zarządzanie eksploatacją pociągu. Porozumienia umowne (na które zwykle składają się umowy ramowe, porozumienia szczególne i załączniki) stanowią podstawę skutecznej współpracy między

różnymi przedsiębiorstwami kolejowymi, zarówno między nowymi operatorami, jak i operatorami dotychczasowymi, i muszą być zgodne z przepisami prawodawstwa unijnego i krajowego oraz ze wszelkimi innymi wymogami mającymi zastosowanie.

W związku z tym przedsiębiorstwo kolejowe musi kontrolować ryzyko wynikające z jego działalności, w tym wynikające ze współpracy z partnerami oraz z korzystania usług (pod)wykonawców. Krajowy organ ds. bezpieczeństwa sprawuje natomiast nadzór nad tym, czy przedsiębiorstwo kolejowe wypełnia swoje zobowiązania prawne w sposób przejrzysty i sumienny.

Przedsiębiorstwa kolejowe nie mogą zlecić swoich obowiązków dotyczących bezpieczeństwa koordynacji i zarządzania bezpieczną eksploatacją pociągów w ramach outsourcingu. Nie ma to jednak negatywnego wpływu na istnienie systemów współpracy między przedsiębiorstwami kolejowymi. Podstawowe zasady wymienione powyżej mają również zastosowanie do współpracy między przedsiębiorstwami kolejowymi. Przedsiębiorstwo kolejowe odpowiedzialne za zapewnienie bezpiecznej eksploatacji pociągów musi posiadać jednolity certyfikat bezpieczeństwa, przy czym należy jasno wymienić we wszystkich umowach zawieranych przez zainteresowane strony. Wspomniane przedsiębiorstwo kolejowe bezpośrednio zarządza zasobami (pracownikami, pojazdami) za pośrednictwem systemu zarządzania bezpieczeństwem albo może podjąć decyzję o zleceniu podwykonawstwa (częściowo lub w całości) w zakresie zarządzania zasobami (np. dzierżawy pojazdów, zatrudniania maszynistów) innej stronie. W tym drugim przypadku przedsiębiorstwo kolejowe nadal ponosi odpowiedzialność za kontrolowanie ryzyka związanego z korzystaniem z usług (pod)wykonawców poprzez monitorowanie wykonywania umowy za pośrednictwem systemu zarządzania bezpieczeństwem zgodnie z [rozporządzeniem \(UE\) nr 1078/2012](#), w związku z czym przedmiotowe przedsiębiorstwo kolejowe musi sprawdzać, czy zasoby te spełniają prawne i inne mające zastosowanie wymogi dotyczące bezpieczeństwa (np. pociągi w stanie umożliwiającym bezpieczną eksploatację, kompatybilność tras, szkolenie personelu, maszyniści posiadający ważną licencję i certyfikat na konkretną trasę).

Dostarczenie kontrahentowi (tj. partnerowi lub podwykonawcy) jednolitego certyfikatu bezpieczeństwa (odpowiednio nadzorowanego przez krajowy organ ds. bezpieczeństwa) przez organ wydający certyfikat bezpieczeństwa może stanowić wystarczające zapewnienie dla odpowiedzialnego za bezpieczny stan eksploatacji przedsiębiorstwa kolejowego, że ustalenia systemu zarządzania bezpieczeństwem spełniają odpowiednie wymogi. Ustalenia umowne obejmują przekazywanie informacji istotnych dla bezpieczeństwa (np. poprzedni czas odpoczynku maszynistów) między kontrahentami.

Zasady stanowiące podstawę współpracy między przedsiębiorstwami kolejowymi pozostają bez zmian bez względu na systemy współpracy, tj. działania kolejowe podejmowane w ramach partnerstwa lub podwykonawstwa (częściowego lub całościowego) podczas działalności krajowej bądź transgranicznej. Charakter i zakres środków, które przedsiębiorstwa kolejowe mają wprowadzić, oraz zakres, w którym krajowy organ ds. bezpieczeństwa musi nadzorować te ustalenia dotyczące współpracy, są jednak proporcjonalne do stopnia współpracy między przedsiębiorstwami kolejowymi.

Przykładowo transgraniczna współpraca między przedsiębiorstwami (tj. korzystanie z zewnętrznych pojazdów lub pracowników) prawdopodobnie wymagać będzie większej kontroli niż każdy inny system współpracy, ponieważ działania przekazuje się innemu przedsiębiorstwu kolejowemu, posługującemu się różnymi językami i zasadami funkcjonowania taboru kolejowego, które mogą różnić się między państwami członkowskimi. Z drugiej strony zatrudnianie wyłącznie zewnętrznych maszynistów lub wynajmowanie zewnętrznych pojazdów oczywiście wymagałoby mniej czynnego monitorowania, a co za tym idzie, mniejszej ilości działań nadzorczych ze strony krajowego organu ds. bezpieczeństwa.

## Załącznik 4 – Kultura bezpieczeństwa

### ***Wprowadzenie do kultury bezpieczeństwa oraz strategia poprawy kultury bezpieczeństwa***

Kultura powstaje w wyniku interakcji ludzi w ich codziennym życiu; pomaga określić oczekiwania względem zachowania oraz normy w społeczeństwie. Kultura jest złożonym pojęciem, w skład którego wchodzi wiele czynników, które zmieniają się w czasie w zależności od okoliczności, środowiska i doświadczeń narodu, państwa, społeczeństwa lub organizacji.

Kultura bezpieczeństwa odnosi się do elementów kultury, które konkretnie nawiązują do bezpieczeństwa. Chociaż możliwe jest przedstawienie niektórych czynników przyczyniających się do tworzenia kultury bezpieczeństwa, nie można zgromadzić wszystkich informacji odzwierciedlających kulturę bezpieczeństwa. Nie ma jednej naukowej miary kultury bezpieczeństwa. Jest tak ze względu na fakt, że składające się na nią czynniki różnią się, nie tylko między organizacjami, ale również w ich obrębie. Różne wydziały mają różne wymagania dotyczące bezpieczeństwa i różne potrzeby, np. operacyjne czy finansowe, i to na ich podstawie powstaje dominująca kultura bezpieczeństwa. Czynniki zewnętrzne, takie jak wymagania regulacyjne, poziom wykształcenia, struktura społeczna i kultura narodowa, również wniosą wkład w kulturę bezpieczeństwa organizacji.

Kultura bezpieczeństwa jest utartym pojęciem. Brakuje jej jednak zgodnej definicji. W tym kontekście Agencja, wraz z przedstawicielami sektora, opracowała następującą definicję mającą zastosowanie do każdej organizacji kolejowej: *Pojęcie kultury bezpieczeństwa odnosi się do wzajemnego oddziaływania wymogów systemu zarządzania bezpieczeństwem (ang. safety management system, SMS), ich rozumienia przez zainteresowane osoby, wynikającego z postaw, wyznawanych wartości i przekonań tych osób oraz podejmowanych przez nie działań, tj. decyzji i zachowań.*

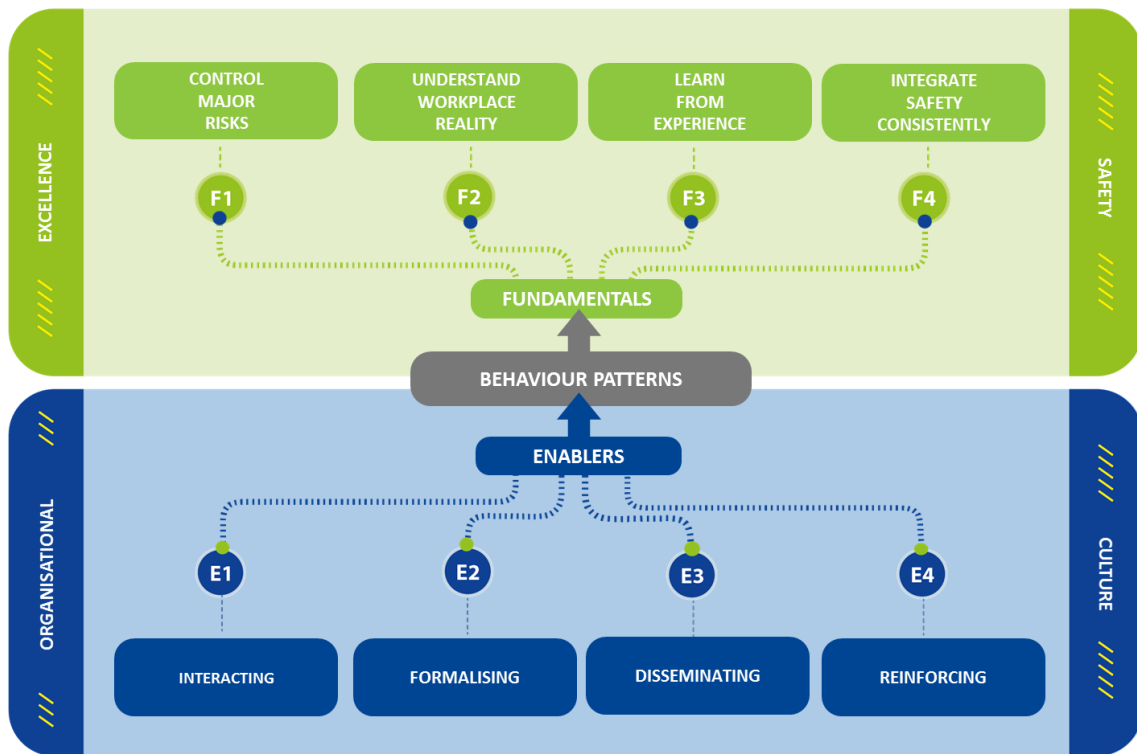
Podsumowując, aby w prosty sposób opisać kulturę bezpieczeństwa, należy przyrzeć się czynnikom kształtującym zachowanie. System zarządzania bezpieczeństwem zapewnia podstawę, określając i wytyczając wymagania za pośrednictwem polityki i procedur. W utopijnym świecie system zarządzania bezpieczeństwem byłby idealny, a cały zarząd i personel przestrzegałby go. Niestety, utopia pozostaje utopią – w rzeczywistości zarząd i personel stara się zinterpretować treść systemu zarządzania bezpieczeństwem na podstawie własnych wartości, postaw i przekonań wynikających z osobistego doświadczenia w połączeniu z normami zachowania w miejscu pracy i w społeczeństwie. Jeżeli system zarządzania bezpieczeństwem jest zasadny i jeżeli istnieje kultura zgodności, następstwem będą poprawne zachowania. W przeciwnym wypadku powstaną indywidualne interpretacje i stosowane będą alternatywne rozwiązania. Będą się one opierać na indywidualnej ocenie ryzyka ważącej czynniki, które wpływają na podjętą decyzję. Taka ocena ryzyka nie tylko będzie skupiać się na faktycznym ryzyku, ale uwzględni również czynniki związane z dogodnością, ryzykiem zostania przyłapanym, słowami i działaniami zarządu itp. Współzależność między systemem zarządzania bezpieczeństwem, dostrzeganiem sensu i zachowaniem przeczy zatem kulturze bezpieczeństwa.

Ocena kultury bezpieczeństwa wymaga zrozumienia tych trzech czynników i współzależności między nimi. Jak wcześniej wspomniano, nie ma jednej naukowej miary kultury bezpieczeństwa. Można natomiast poddać analizie cechy charakterystyczne, które mają wpływ na rozwój kultury bezpieczeństwa, opierając się na tych trzech czynnikach.

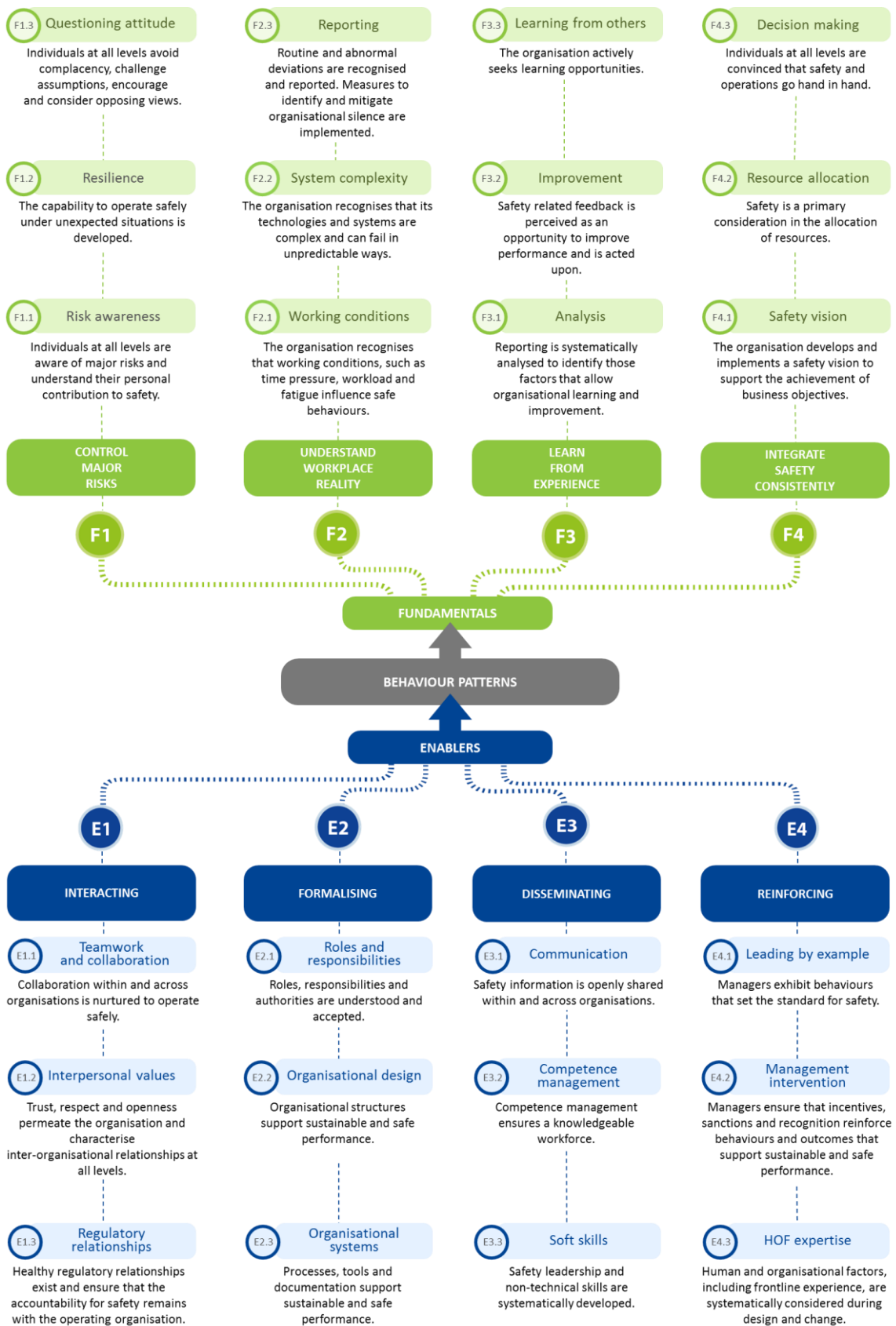
Na przykład oświadczenie, takie jak „Bezpieczeństwo przede wszystkim” można rozszerzyć o zbadanie, co oznacza ono dla pracowników – czy faktycznie w nie wierzą, czy zarząd „wie co robi”, jak i na jakich podstawach podejmowane są decyzje, jak organizacja reaguje na nacisk itp. Podobne badania można przeprowadzić, uwzględniając inne czynniki, takie jak stałe uczenie się i postawa krytyczna. Połączone wyniki analizy przedstawią obecny stan kultury. Z biegiem czasu można stworzyć bardziej kompleksowy obraz sytuacji, umożliwiając wyciągnięcie dokładniejszych wniosków.



Europejski Kolejowy Model Kultury Bezpieczeństwa (zob. Rys. 4) został opracowany jako ramy koncepcyjne i ramy oceny, które można wykorzystać do lepszego zrozumienia pojęcia kultury bezpieczeństwa oraz do oceny i poprawy kultury bezpieczeństwa każdej organizacji kolejowej.



Rys. 4: Europejski Kolejowy Model Kultury Bezpieczeństwa



Rys.5: Cechy Europejskiego Kolejowego Modelu Kultury Bezpieczeństwa

## Porównanie wymogów dotyczących systemu zarządzania bezpieczeństwem i Europejskiego Kolejowego Modelu Kultury Bezpieczeństwa

W poniższych tabelach przedstawiono porównanie fundamentów i uwarunkowań Europejskiego Kolejowego Modelu Kultury Bezpieczeństwa oraz wymogów dotyczących systemu zarządzania bezpieczeństwem określonych w [rozporządzeniu \(UE\) 2018/762](#).

Uważne korzystanie z tabel wraz z [wytycznymi dotyczącymi modelu kultury bezpieczeństwa kolei europejskich](#) powinno umożliwić organizacji dostrzeżenie, które z wymogów dotyczących systemu zarządzania bezpieczeństwem są ściśle powiązane z cechami modelu kultury bezpieczeństwa kolei europejskich, a tym samym pozwolić na opracowanie procesów i procedur, które lepiej uwzględniają pożądane zachowania organizacyjne.

*Tabela 6: Porównanie – wymogi dotyczące systemu zarządzania bezpieczeństwem/Europejski Kolejowy Model Kultury Bezpieczeństwa*

| <i>Wymóg dotyczący systemu zarządzania bezpieczeństwem</i>                      | <i>Powiązanie z cechami Europejskiego Kolejowego Modelu Kultury Bezpieczeństwa</i>   |
|---|--|
| 1. Kontekst organizacji   | F1.1, F2.2, F3.3 F4.1<br>E1.1, E2.1, E2.2, E3.1, E4.3  |
| 2.1 Przywództwo i zaangażowanie   | F1.1, F2.1, F2.2, F4.1<br>E1.1, E2.1, E3.1   |
| 2.2 Strategia w zakresie bezpieczeństwa   | F1.1, F2.1, F2.2, F4.1<br>E1.1, E3.1   |
| 2.3 Funkcje, odpowiedzialność, rozliczalność i uprawnienia w ramach organizacji | F1.1, F2.1, F2.2, F2.3, F3.1, F 3.2, F4.1, F4.2<br>E1.1, E2.1, E2.2, E3.1, E3.2, E4.3  |
| 2.4 Konsultacje z pracownikami i innymi stronami                                | F1.1, F2.1, F2.2, F2.3, F3.1, F3.2, F4.1, F4.2,<br>E1.1, E2.2, E2.3, E3.1, E4.3  |
| 3.1 Działania mające na celu ograniczenie ryzyka                                | F1.1, F2.1, F2.2, F2.3, F3.1, F3.2 F3.3, F4.1, F4.3<br>E1.1, E2.1, E2.2, E2.3, E3.1, E3.2, E4.3                                |
| 3.2 Cele w zakresie bezpieczeństwa i planowanie                                 | F1.1, F2.1, F2.2, F2.3, F3.1, F 3.2, F4.1, F4.2<br>E1.1, E2.2, E2.3, E3.1, E4.3  |
| 4.1 Zasoby  | F1.1, F2.1, F2.2, F4.1, F4.2,<br>E1.1, E1.2, E2.1, E2.2, E2.3, E3.1, E3.2, E3.3, E4.3  |
| 4.2 Kompetencje   | F1.1, F1.2, F1.3, F2.1, F2.2, F2.3, F3.1, F3.2, F4.1, F4.2, F4.3<br>E1.1, E2.1, E2.2, E2.3, E3.1, E3.2, E3.3, E4.1, E4.2, E4.3 |
| 4.3 Świadomość  | F1.1, F1.2, F2.2, F2.3, F3.1, F3.2, F4.1, F4.3<br>E1.1, E1.2, E2.1, E3.1, E3.2, E3.3, E4.1, E4.2                               |
| 4.4 Informowanie i komunikowanie  | F1.1, F1.2, F2.2, F2.3, F3.1, F3.2, F4.1, F4.3<br>E2.1, E3.1, E3.2, E3.3, E4.2   |
| 4.5 Dokumentacja  | F1.1, F1.2, F2.2, F2.3, F3.1, F3.2, F4.1, F4.3<br>E2.1, E2.2, E2.3, E3.1, E3.2, E3.3, E4.2                                     |
| 4.6 Integracja czynników ludzkich i organizacyjnych                             | F1.1, F1.2, F2.2, F2.3, F3.1, F3.2, F4.1, F4.3<br>E2.1, E2.2, E2.3, E3.1, E3.2, E3.3, E4.3                                     |
| 5.1 Planowanie operacyjne i kontrola operacyjna                                 | F1.1, F2.1, F2.2, F3.1, F3.2, F4.1, F4.2<br>E2.1, E2.3, E3.1, E3.2, E3.3, E4.3   |
| 5.2 Zarządzanie składnikami aktywów   | F2.1, F2.2, F4.1, F4.2, F4.3,<br>E1.1, E2.3, E3.1, E3.2, E4.3  |
| 5.3 Wykonawcy, partnerzy i dostawcy   | F1.1, F2.1, F2.2, F4.1, F4.2, F4.3<br>E1.1, E2.3, E3.1, E3.2, E4.3   |

| <i>Wymóg dotyczący systemu zarządzania bezpieczeństwem</i> | <i>Powiązanie z cechami Europejskiego Kolejowego Modelu Kultury Bezpieczeństwa</i>                                       |
|--|--|
| 5.4 Zarządzanie zmianą                                     | F1.1, F2.1, F2.2, F4.1, F4.2, F4.3<br>E1.1, E2.3, E3.1, E3.2, E4.3   |
| 5.5 Zarządzanie sytuacjami kryzysowymi                     | F1.1, F1.2, F1.3, F2.1, F2.2, F3.1, F3.2, F3.3, F4.1, F4.2, F4.3<br>E1.1, E2.3, E3.1, E3.2, E3.3, E4.1, E4.2, E4.3       |
| 6.1. Monitorowanie   | F1.1, F1.2, F1.3, F2.1, F2.2, F3.1, F3.2, F4.1, F4.2, F4.3<br>E1.1, E1.2, E2.1, E2.3, E3.1, E3.2, E3.3, E4.1, E4.2, E4.3 |
| 6.2 Audyt wewnętrzny                                       | F1.1, F1.2, F1.3, F2.1, F2.2, F3.1, F3.2, F4.1, F4.2, F4.3<br>E1.1, E2.1, E2.3, E3.1, E3.2, E3.3, E4.1, E4.2, E4.3       |
| 6.3. Przegląd dokonywany przez kierownictwo                | F1.1, F1.2, F1.3, F2.1, F2.2, F3.1, F3.2, F4.1, F4.2, F4.3<br>E1.1, E2.1, E2.3, E3.1, E3.2, E3.3, E4.1, E4.2, E4.3       |
| 7.1. Wyciąganie wniosków z wypadków i incydentów           | F1.1, F1.3, F2.1, F2.2, F2.3, F3.1, F3.2, F4.1, F4.3<br>E1.3, E2.1, E2.3, E3.1, E3.2, E3.3, E4.2, E4.3                   |
| 7.2. Ciągłe doskonalenie                                   | F1.1, F1.3, F2.1, F2.2, F2.3, F3.1, F3.2, F4.1, F4.3<br>E2.1, E2.3, E3.1, E3.2, E3.3, E4.2, E4.3                         |

*Tabela 7: Porównanie – Europejski Kolejowy Model Kultury Bezpieczeństwa/wymogi dotyczące systemu zarządzania bezpieczeństwem*

| <i>Cechy Europejskiego Kolejowego Modelu Kultury Bezpieczeństwa</i> | <i>Powiązanie z wymogiem dotyczącym systemu zarządzania bezpieczeństwem</i>                                     |
|---|---|
| F 1.1 Świadomość ryzyka   | 1, 2.1, 2.2, 2.3, 2.4, 3.1, 3.2, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2 |
| F1.2 Odporność  | 4.1, 4.2, 4.3, 4.5, 4.6, 5.5, 6.1, 6.2, 6.3   |
| F1.3 Poddawanie w wątpliwość  | 5.5, 6.1, 6.2, 6.3, 7.1, 7.2  |
| F2.1 Warunki pracy  | 2.1, 2.2, 2.3, 2.4, 3.1, 3.2, 4.1, 4.2, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2                        |
| F2.2 Złożoność systemu  | 1, 2.1, 2.2, 2.3, 2.4, 3.1, 3.2, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2 |
| F2.3 Sprawozdawczość  | 2.3, 2.4, 3.2, 4.2, 4.3, 4.4, 4.5, 4.6, 7.1, 7.2  |
| F3.1 Analiza  | 2.3, 2.4, 3.2, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2                                       |
| F3.2 Doskonalenie   | 2.3, 2.4, 3.2, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2                                       |
| F3.3 Uczenie się od innych osób                                     | 3.1, 5.5  |
| F4.1 Wizja bezpieczeństwa   | 1, 2.1, 2.2, 2.3, 2.4, 3.1, 3.2, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2 |
| F4.2 Przydział zasobów  | 2.3, 2.4, 3.2, 4.1, 4.2, 5.1, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3  |
| F4.3 Podjęcie decyzji   | 3.1, 3.2, 4.2, 4.3, 4.4, 4.5, 4.6, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2, 7.3                             |
| E1.1 Praca zespołowa i współpraca                                   | 1, 2.1, 2.2, 2.3, 2.4, 3.1, 3.2, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2 |
| E1.2 Wartość interpersonalna  | 4.1, 4.3, 6.1   |
| E1.3 Stosunek regulacyjny   | 7.1   |
| E2.1 Role i zadania   | 1, 2.1, 2.3, 3.1, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 6.1, 6.2, 6.3, 7.1, 7.2                                    |
| E2.2 Projektowanie organizacyjne                                    | 1, 2.1, 2.3, 2.4, 2.4, 3.1, 3.2, 4.1, 4.2, 4.4, 4.5   |
| E2.3 Systemy organizacyjne  | 2.4, 3.1, 3.2, 4.1, 4.2, 4.5, 4.6, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2                             |

| <i>Cechy Europejskiego Kolejowego Modelu Kultury Bezpieczeństwa</i> | <i>Powiązanie z wymogiem dotyczącym systemu zarządzania bezpieczeństwem</i>                                  |
|---|--|
| E3.1 Komunikacja  | 2.1, 2.2, 2.3, 2.4, 3.1, 3.2, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2 |
| E3.2 Zarządzanie kompetencjami                                      | 3.1, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2                          |
| E3.3 Umiejętności miękkie   | 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 6.1, 6.2, 6.3, 7.1, 7.2   |
| E4.1 Służenie przykładem  | 4.2, 4.3, 5.5, 6.1, 6.2, 6.3   |
| E4.2 Interwencja w zakresie zarządzania                             | 4.2, 4.3, 4.4, 4.5, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2   |
| E4.3 Wiedza fachowa z zakresu czynników ludzkich i organizacyjnych  | 1, 2.3, 2.4, 3.1, 3.2, 4.1, 4.2, 4.6, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 7.1, 7.2                       |

Dodatkowe informacje na temat kultury bezpieczeństwa można znaleźć na [stronie internetowej ERA](#)

## Załącznik 5 – Czynniki ludzkie i organizacyjne

### ***Wprowadzenie do czynników ludzkich i organizacyjnych***

Czynniki ludzkie i organizacyjne to multidyscyplinarna dziedzina zajmująca się sposobami zwiększenia bezpieczeństwa, podniesienia wydajności i zwiększenia zadowolenia użytkownika. Czynniki ludzkie i organizacyjne stanowią podejście skupione na użytkowniku, tzn. projekt opiera się na dogłębnym zrozumieniu użytkownika, zadań i środowisk. Punktem początkowym zawsze są zdolności i ograniczenia użytkownika oraz sposób, w jaki są podatne i w jaki reagują z systemami napotykanymi podczas wykonywania zadań. Celem jest zidentyfikowanie, jak wykonać zadanie w sposób bezpieczny i skuteczny. Nacisk kładzie się na funkcjonalność. Czynniki ludzkie i organizacyjne stosuje się zarówno jako zapobiegawcze środki zapewniania dobrych procesów projektu, jak również jako reaktywne środki identyfikacji głównych problemów w przypadku, gdy coś pójdzie nie tak.

Podczas np. projektowania nowych pojazdów nie wystarczy zastosować jedynie standardów konstrukcyjnych. Maszyniści, konduktorzy i pracownicy odpowiedzialni za utrzymanie powinni być zaangażowani, aby wnieść swoje doświadczenia i zrozumienie sposobu wykonywania zadań bezpiecznie i skutecznie. Może to być np. związane z kwestiami dotyczącymi konkretnej stacji lub linii, dostępnością i dostępem dla pracowników odpowiedzialnych za utrzymanie, zadaniami priorytetowymi w kabinie, wymogami w zakresie komunikacji lub zachowaniami pasażerów na stacjach.

Wiedzę i doświadczenie różnych operatorów najlepiej pozyskuje się w drodze metody iteracyjnej, w ramach której użytkownik stale ocenia projekt i budowę pociągu podczas postępów w jego projekcie i budowie. Pomaga to zapobiec powszechnym błędom w procesie projektowania, tzn. pomaga skupić się na interakcji człowieka z indywidualnymi systemami, nie na wykonywaniu zadań w ogóle. Przykładowo różni dostawcy mają różne poglądy na to, w jaki sposób należy przyznawać priorytety alarmom, a bez całościowej perspektywy użytkownik często jest nadmiernie obciążony informacjami o ograniczonej przydatności dla wykonywania zadania. Użytkownik nie musi mieć potrzeby korzystania z takich informacji tylko dlatego, że projekt techniczny daje możliwość ich wyświetlenia. Analiza czynników ludzkich i organizacyjnych pomaga zdecydować, które informacje są potrzebne, a które nie są niezbędne.

Zagadnienie czynników ludzkich i organizacyjnych uwzględnia także spojrzenie systemowe, tzn. w jego ramach nie rozpatruje się czynników ludzkich, technologicznych i organizacyjnych jako takich, za to nacisk kładzie się na interakcje między poszczególnymi czynnikami. Na przykład, jeżeli maszynista brał udział w incydencie, takim jak zignorowanie sygnału ostrzegawczego, sugeruje się zbadanie czynników (lista nie jest wyczerpująca) związanych ze zmęczeniem, z przeładowaniem sensorycznym, kompetencjami, itp. (czynniki ludzkie); wpływem technologii na skuteczność, np. interakcji między człowiekiem i systemem, rozkładem, rozmieszczeniem sygnałów (czynniki technologiczne); wpływem organizacji na funkcjonowanie, np. szkolenia, system zarządzania bezpieczeństwem, priorytety organizacyjne (czynniki organizacyjne); a także interakcje między tymi trzema obszarami, takie jak wpływ kwestii związanych z zamawianiem na projektowanie lub zarządzanie zmianą po wprowadzeniu nowego projektu.

Metody ustala się na podstawie wielu różnych dziedzin, np. psychologii eksperymentalnej, inżynierii przemysłowej, psychologii organizacji, socjologii, nauki o zarządzaniu, inżynierii kognitywnej, ergonomii, informatyki i inżynierii bezpieczeństwa.

Ze względu na fakt, że waga zagadnienia czynników ludzkich i organizacyjnych spoczywa na użytkowniku, powszechnie stosowaną metodą jest analiza zadań. Analiza zadań pozwala projektantom zrozumieć zadania, które należy wykonać, i w jaki sposób odnoszą się one do systemów, z którymi użytkownik ma styczność, oraz do warunków organizacyjnych, które mają wpływ na wyniki. Na podstawie analizy zadań można przeprowadzić kolejne analizy, takie jak analiza interakcji między człowiekiem i systemem, obciążenia pracą, niezawodności/ryzyka ludzkiego, antropometrii i biometrii. Zasadnicze znaczenie ma zapewnienie użytkownikowi najlepszych możliwych warunków pracy pod kątem bezpiecznych i skutecznych wyników.

Dodatkowe informacje dotyczące czynników ludzkich i organizacyjnych można znaleźć na [stronie internetowej ERA](#).

## **Strategia na rzecz wsparcia integracji czynników ludzkich i organizacyjnych z systemem zarządzania bezpieczeństwem**

Organizacja powinna zapewnić strategię, aby mieć pewność, że związane z czynnikami ludzkimi wiedza i metody oraz podejście zorientowane na człowieka są systematycznie i konsekwentnie stosowane w stosunku do istotnych procesów w obrębie organizacji. Takie podejście oznacza uwzględnienie przede wszystkim potrzeb, zdolności i zachowań ludzi, a następnie planowanie w taki sposób, aby wziąć pod uwagę te potrzeby, zdolności i zachowania.

Wśród elementów zawartych w strategii dotyczącej czynników ludzkich i organizacyjnych mogą znajdować się:

### **Przywództwo**

- *Przywództwo i zaangażowanie*
  - *zobowiązanie zarządu do uwzględniania czynników ludzkich i organizacyjnych jest wyraźnie zaznaczone w polityce i celach;*
  - *istnieje proces lub wytyczne wskazujące, w jaki sposób zagadnienie czynników ludzkich i organizacyjnych należy stosować w projektach;*
  - *zagadnienie czynników ludzkich i organizacyjnych jest integralną częścią procesu projektowania oraz zarządzania projektem.*
- *Strategia w zakresie bezpieczeństwa*
  - *w strategii w zakresie bezpieczeństwa jest wyraźnie zaznaczone, że perspektywę czynników ludzkich i organizacyjnych należy stosować we wszystkich procesach związanych z bezpieczeństwem.*
- *Funkcje, odpowiedzialność, rozliczalność i uprawnienia w ramach organizacji*
  - *funkcje, odpowiedzialność, rozliczalność i uprawnienia specjalistów ds. czynników ludzkich i organizacyjnych są jasno określone;*
  - *istnieje proces określający, w jaki sposób eksperci ds. czynników ludzkich i organizacyjnych mogą regularnie uczestniczyć w projektach i procesach.*

### **Planowanie**

- *Działania mające na celu ograniczenie ryzyka*
  - *opis sposobu, w jaki perspektywę czynników ludzkich i organizacyjnych uwzględnia się w analizach ryzyka;*
  - *zaangażowanie specjalistów i pracowników pierwszej linii ds. czynników ludzkich i organizacyjnych, w tym osób mających styczność z analizami ryzyka*

### **Wsparcie**

- *Zasoby i kompetencje*
  - *systematyczne podejście polegające na wykorzystaniu kompetencji w zakresie czynników ludzkich i organizacyjnych w celu zapewnienia, by role związane z bezpieczeństwem miały wystarczające zasoby w oparciu o ocenę ryzyka;*
  - *powiązanie między oceną ryzyka, zadaniami związanymi z bezpieczeństwem i systemem zarządzania kompetencjami, aby zapewnić, że personel stale posiada wymagane kompetencje;*
  - *przeznaczenie czasu i zasobów, aby zapewnić spełnienie wymogów w zakresie czynników ludzkich i organizacyjnych.*
- *Świadomość*
  - *systematyczne wykorzystywanie kompetencji w zakresie czynników ludzkich i organizacyjnych w organizacji w celu zapewnienia, by personel wykonujący odpowiednie funkcje był świadomy roli, jaką odgrywa w dziedzinie bezpieczeństwa.*



**Działalność**

- *Planowanie operacyjne i kontrola operacyjna*
  - *zagadnienia z zakresu czynników ludzkich i organizacyjnych bierze się pod uwagę w planowaniu operacyjnym.*
- *Zarządzanie składnikami aktywów*
  - *organizacja posiada wytyczne dotyczące stosowania podejścia zorientowane na człowieka na każdym etapie cyklu życia.*
- *Zarządzanie zmianą*
  - *czynniki ludzkie i organizacyjne zawsze ocenia się jako część procesu zarządzania zmianą.*

**Ocena wyników**

- *Monitorowanie*
  - *skuteczność działania w zakresie bezpieczeństwa jest oceniana systematycznie, w świetle strategii w zakresie czynników ludzkich i organizacyjnych.*

**Doskonalenie**

- *Wyciąganie wniosków z wypadków i incydentów*
  - *wiedza fachowa i metody z zakresu czynników ludzkich i organizacyjnych wykorzystuje się w procesie dochodzenia w sprawie wypadku;*
  - *istnieje metodyka prowadzenia dochodzeń na podstawie wiedzy i metod z zakresu czynników ludzkich i organizacyjnych;*
  - *istnieje program szkoleniowy dla osób prowadzących dochodzenia w sprawie wypadków i incydentów, w ramach którego stosuje się perspektywę zagadnienia czynników ludzkich i organizacyjnych.*
- *Ciągłe doskonalenie*
  - *proces stałego doskonalenia procesów organizacji w zakresie zarządzania czynnikami ludzkimi i organizacyjnymi.*

**Załącznik 6 – Definicje**

Zastosowanie słów lub terminów takich jak „należy”, „powinien” lub „musi” w niniejszym dokumencie wskazuje na istnienie wymogu prawnego, zachowanie zgodności z którym jest konieczne. Definicje zawarte w powiązanych przepisach dotyczących bezpieczeństwa kolei, takich jak dyrektywa (UE) 2016/798 w sprawie bezpieczeństwa kolei, rozporządzenie (UE) nr 402/2013 w sprawie wspólnej metody oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka oraz w odpowiednich technicznych specyfikacjach interoperacyjności, mają zastosowanie do niniejszego dokumentu, ale nie zostały przytoczone poniżej.

|                                 |  |
|---------------------------------|--|
| Wypadek                         | Niechciane lub niezamierzone nagłe zdarzenie lub ciąg takich zdarzeń, które mają dotkliwe konsekwencje; wypadki dzielą się na następujące kategorie: kolizje, wykolejenia, wypadki na przejazdach, wypadki z udziałem osób dotyczące taboru kolejowego będącego w ruchu, pożary i inne (dyrektywa (UE) 2016/798).  |
| Obszar działalności             | Sieć lub sieci w państwie członkowskim lub państwach członkowskich, w którym lub w których przedsiębiorstwo kolejowe zamierza prowadzić działalność (dyrektywa (UE) 2016/798).   |
| Zarządzanie składnikami aktywów | Podejście przyjęte przez organizację w celu zapewnienia, aby fizyczne składniki aktywów pozostały bezpieczne, odpowiednie do celu i ekonomicznie opłacalne od momentu projektu i konstrukcji przez cały swój cykl życia, aż do likwidacji.   |
| Audyt                           | Systematyczny, niezależny i udokumentowany proces prowadzący do uzyskania dowodu z audytu i jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu (ISO 9000).   |
| Jednostka gospodarcza           | Jednostka gospodarcza to dział lub obszar funkcjonalny w organizacji. Może dotyczyć różnych ról i celów, np. zasobów ludzkich, produkcji, transportu na duże odległości, logistyki, manewrowania.  |
| Charakter działalności          | Scharakteryzowanie działalności poprzez jej zakres, obejmujący projektowanie i budowę infrastruktury, utrzymanie infrastruktury, planowanie ruchu oraz zarządzanie i sterowanie ruchem, oraz poprzez wykorzystanie infrastruktury kolejowej, obejmujące linie konwencjonalne lub linie dużych prędkości oraz przewóz osób lub towarów.   |
| Kompetencje                     | Zdolność zastosowania wiedzy i umiejętności w celu osiągnięcia zamierzonych rezultatów (ISO 9000).   |
| Ciągłe doskonalenie             | Powtarzalna działalność poprawiająca wyniki (np. mierzalne wyniki) (ISO 9000).   |
| Zarządzanie dokumentami         | Proces (lub procedura) identyfikacji, tworzenia, utrzymywania, zarządzania, przechowywania i zatrzymywania dokumentacji.   |
| Zakres działalności             | W odniesieniu do działalności kolejowej prowadzonej przez przedsiębiorstwa kolejowe: zakres określany w kategoriach liczby pasażerów lub wolumenu towarów oraz szacunkowej wielkości przedsiębiorstwa kolejowego wyrażonej liczbą pracowników pracujących w sektorze kolejowym (tj. mikroprzedsiębiorstwo, małe, średnie albo duże przedsiębiorstwo) (dyrektywa (UE) 2016/798).<br><br>W odniesieniu do działalności kolejowej prowadzonej przez zarządców infrastruktury: zakres scharakteryzowany przez długość torów linii kolejowych oraz szacowaną wielkość zarządcy infrastruktury pod względem liczby jego pracowników zatrudnionych w sektorze kolejowym (rozporządzenie (UE) 2018/762). |

|                                     |   |
|-------------------------------------|---|
| Zagrożenie                          | Stan, który może prowadzić do wypadku (rozporządzenie (UE) nr 402/2013).  |
| Czynniki ludzkie i organizacyjne    | Cała charakterystyka działań człowieka i aspektów organizacyjnych, które należy wziąć pod uwagę w celu zapewnienia bezpieczeństwa i skuteczności systemu lub organizacji przez cały jego/jej cykl życia.  |
| Podejście zorientowane na człowieka | Podejście uwzględniające przede wszystkim potrzeby, zdolności i zachowania ludzi, a następnie planowanie w taki sposób, aby wziąć pod uwagę te potrzeby, zdolności i zachowania.  |
| Incydent                            | Każde zdarzenie, inne niż wypadek lub poważny wypadek, mające wpływ na bezpieczeństwo eksploatacji kolei (dyrektywa (UE) 2016/798). Należą do nich wypadki, których uniknięto.  |
| Zarządca infrastruktury             | Każdy podmiot lub przedsiębiorstwo odpowiedzialne w szczególności za stworzenie, zarządzanie i utrzymywanie infrastruktury kolejowej, w tym za zarządzanie ruchem i podsystemem Sterowanie; funkcja zarządcy infrastruktury sieci lub jej części może być przydzielona różnym podmiotom lub przedsiębiorstwom (dyrektywa 2012/34/UE).   |
| Zainteresowana strona               | Osoba lub organizacja, która może mieć wpływ na decyzję lub działalność związaną z systemem zarządzania bezpieczeństwem, na którą taka decyzja lub działalność może mieć wpływ lub która może uznać, że taka decyzja lub działalność ma na nią wpływ (ISO 9000).  |
| Dochodzenie                         | Proces realizowany w celu zapobiegania wypadkom i incydentom, obejmujący zbieranie i analizę informacji, wyciąganie wniosków, łącznie z ustaleniem przyczyn, oraz, gdzie to właściwe, opracowanie zaleceń w zakresie bezpieczeństwa (dyrektywa (UE) 2016/798).  |
| System zarządzania                  | Zbiór wzajemnie powiązanych lub wchodzących ze sobą w interakcje elementów organizacji mających na celu ustanowienie polityki i celów oraz procesy służące osiągnięciu tych celów (ISO 9000).   |
| Monitorowanie                       | Rozwiązania wprowadzone przez przedsiębiorstwa kolejowe, zarządców infrastruktury lub podmioty odpowiedzialne za utrzymanie w celu kontrolowania prawidłowego stosowania i skuteczności własnego systemu zarządzania (rozporządzenie (UE) nr 1078/2012).  |
| Przepisy krajowe                    | Wszystkie wiążące przepisy przyjęte w państwie członkowskim, niezależnie od tego, jaki organ je wydał, obejmujące wymogi dotyczące bezpieczeństwa kolei lub wymogi techniczne, inne niż wymogi nałożone przez Unię lub przepisy międzynarodowe, i które mają zastosowanie w tym państwie członkowskim do przedsiębiorstw kolejowych, zarządców infrastruktury lub stron trzecich (dyrektywa (UE) 2016/798). |
| Proces                              | Zbiór wzajemnie powiązanych lub wchodzących ze sobą w interakcje działań, które przekształcają dane wejściowe w wyniki (ISO 9000).  |

|                           |  |
|---------------------------|--|
| Infrastruktura kolejowa   | <p>Infrastruktura niezbędna do umożliwienia eksploatacji kolei, w tym:</p> <ul style="list-style-type: none"> <li>tory kolejowe i powiązane z nimi struktury;</li> <li>drogi serwisowe, systemy sygnalizacyjne, systemy komunikacyjne, tabor kolejowy;</li> <li>systemy kontroli, systemy sterowania pociągami i systemy zarządzania danymi;</li> <li>ostrzeżenia i znaki;</li> <li>system zasilania elektrycznego i system trakcji elektrycznej;</li> <li>powiązane budynki, warsztaty, zajezdnie, stacje; oraz</li> <li>zakłady, maszyny i sprzęt.</li> </ul>  |
| Przedsiębiorstwo kolejowe | <p>Przedsiębiorstwo kolejowe zdefiniowane w art. 3 pkt 1 dyrektywy 2012/34/UE oraz każde inne przedsiębiorstwo publiczne lub prywatne, którego działalność polega na wykonywaniu kolejowych przewozów towarowych lub pasażerskich z zastrzeżeniem, że przedsiębiorstwo to ma zapewniać trakcję, łącznie z przedsiębiorstwami, które zapewniają wyłącznie trakcję (dyrektywa (UE) 2016/798).</p> <p>Każde przedsiębiorstwo publiczne lub prywatne, posiadające licencję zgodnie z niniejszą dyrektywą, którego działalność podstawowa polega na świadczeniu usług w transporcie towarowym lub pasażerskim koleją, z zastrzeżeniem, że przedsiębiorstwo to zapewnia pojazdy trakcyjne; obejmuje to także przedsiębiorstwa, które tylko dostarczają pojazdy trakcyjne (dyrektywa 2012/34/UE).</p> |
| Ryzyko                    | Częstotliwość wypadków i incydentów prowadzących do szkody (spowodowanej zagrożeniem) oraz stopień powagi tej szkody (rozporządzenie (UE) 402/2013).   |
| Analiza ryzyka            | Systematyczne wykorzystywanie wszystkich dostępnych informacji do identyfikowania zagrożeń i szacowania ryzyka (rozporządzenie (UE) 402/2013).   |
| Ocena ryzyka              | Całościowy proces obejmujący analizę ryzyka i wycenę ryzyka (rozporządzenie (UE) 402/2013).  |
| Wycena ryzyka             | Procedura opierająca się na analizie ryzyka, która ma na celu ustalenie, czy osiągnięto poziom dopuszczalnego ryzyka (rozporządzenie (UE) 402/2013).   |
| Zarządzanie ryzykiem      | Planowe stosowanie polityki, procedur i praktyk zarządczych w ramach zadań dotyczących analizy, wyceny i nadzoru ryzyka (rozporządzenie (UE) 402/2013).  |
| Kultura bezpieczeństwa    | Wzajemne oddziaływanie wymogów systemu zarządzania bezpieczeństwem, ich rozumienie przez zainteresowane osoby, wynikające z postaw, wyznawanych wartości i przekonań tych osób oraz podejmowanych przez nie działań, tj. decyzji i zachowań. Pozytywna kultura bezpieczeństwa oznacza zaangażowanie kierownictwa i personelu w dbałość o bezpieczeństwo, szczególnie w obliczu sprzecznych celów (rozporządzenie (UE) 2018/762).   |
| Cel                       | <p>Wynik, który ma być osiągnięty.</p> <p>Cel w zakresie bezpieczeństwa musi być skonkretyzowany, mierzalny, osiągalny, realny i terminowy. Musi być również określony na odpowiednich funkcjach i poziomach w ramach organizacji.</p>   |

|                                     |  |
|-------------------------------------|--|
| Partner                             | Podmiot handlowy, z którym inny podmiot handlowy zawarł pewną formę sojuszu. Relacja ta może być umownym zobowiązaniem o charakterze wyłącznym, w którym obie strony zobowiązują się do niezawierania sojuszu z osobami trzecimi.              |
| Partnerstwo                         | Umowa, w której strony określane jako partnerzy zgadzają się współpracować, aby przyspieszyć osiągnięcie swoich wspólnych interesów.   |
| System zarządzania bezpieczeństwem  | Organizacja, środki i procedury przyjęte przez zarządcę infrastruktury lub przedsiębiorstwo kolejowe w celu zapewnienia bezpiecznego zarządzania swoim działaniem (dyrektywa (UE) 2016/798).   |
| Kadra kierownicza wyższego szczebla | Osoba lub grupa ludzi, którzy kierują i kontrolują organizację na najwyższym poziomie (ISO 9000).  |
| Rodzaj działalności                 | Rodzaj charakteryzujący się transportem pasażerskim, obejmujący lub nie przewozy kolejami dużych prędkości, przewozy towarowe, obejmujący lub nie przewozy ładunków niebezpiecznych, a także tylko usługi manewrowe (dyrektywa (UE) 2016/798). |