

Załącznik nr 3 do Ogłoszenia o Wstępnych Konsultacjach Rynkowych

Ogólne założenia Systemu zarządzania ryzykiem operacyjnym

I. System powinien umożliwiać:

1. Określenie procesów, nadanie im kategorii (podstawowy, wspierający, zarządczy), dokonanie podziału w ramach kategorii na krytyczne, istotne.
2. Określenie na podstawie przekazanych przez kierujących komórkami organizacyjnymi CIRF formularzy samooceny ryzyka operacyjnego celów w ramach procesów.
3. Określenie zadań dla realizacji celów w ramach procesów oraz mierników dla tych zadań.
4. Monitoring statusu realizacji zadań dla realizacji celów.
5. Monitoring celów w ramach procesów.
6. Weryfikacja realizacji zadań i celów, ocena stopnia realizacji zadań i celów, wskazanie zagrożeń dla realizacji zadań i celów.
7. Określenie ryzyk dla zadań i celów.
8. Określenie możliwości wystąpienia w ramach danego celu ryzyka inherentnego. Możliwość wystąpienia ryzyka inherentnego oceniana będzie w 5-stopniowej skali prawdopodobieństwa wystąpienia ryzyka i jego skutków. Możliwość wystąpienia ryzyka inherentnego będzie oceniana na podstawie formularzy samooceny ryzyka operacyjnego przekazanych przez kierujących komórkami organizacyjnymi CIRF.
9. Definicja mechanizmów kontrolnych w ramach występujących ryzyk.
10. Przypisanie zdefiniowanych mechanizmów kontrolnych do ryzyk.
11. Możliwość nadania oceny skuteczności dla przypisanych mechanizmów kontrolnych w ramach ryzyk.
12. Określenie ryzyka rezydualnego.
13. Możliwość zmiany oceny ryzyka przez zdefiniowanych użytkowników.
14. Dodawanie nowych ryzyk i ich ocena w kontekście możliwości wystąpienia ryzyka i jego skutków. Możliwość przypisania ryzyka do procesów.
15. Możliwość generowania raportów przez zdefiniowanych użytkowników w dowolnych konfiguracjach z dowolnych okresów.
16. Możliwość prowadzenia bazy wskaźników KRI / KPI, okresowego monitorowania poziomu wskaźników, generowania raportów. Alerty dla przekroczonych limitów wskaźników KRI / KPI.
17. Weryfikacja i ocena skuteczności mechanizmów kontrolnych dla ryzyk.
18. Możliwość tworzenia i aktualizacji mapy ryzyka w sposób graficzny z uwzględnieniem podziału na jednostki organizacyjne.

19. Przygotowanie formularzy samooceny dla ryzyka operacyjnego, ich wysyłka, odbiór i możliwość zaimportowania/przeniesienia danych z formularzy.
20. Udostępnienie interfejsu do raportowania zdarzeń ryzyka operacyjnego poprzez wstępną rejestrację zdarzenia przez użytkownika polegającą na wypełnieniu daty powzięcia informacji o zdarzeniu, opisie skutków i ewentualnie opisie przyczyny (jeśli znana).
21. Pełna rejestracja zdarzenia, w tym konieczność przypisania zgłoszonego zdarzenia do zdefiniowanej listy kategorii ryzyka.
22. Możliwość przypisania skutku finansowego do zgłoszonego zdarzenia z uwzględnieniem straty rzeczywistej, potencjalnej, utraconych korzyści i odzysku.
23. Możliwość aktualizacji skutku finansowego po rejestracji incydentu.
24. Alert dla zgłoszonego zdarzenia jeśli poziom ryzyka jest nieakceptowalny.
25. Możliwość zmiany zdarzenia z otwartego na zamknięte i odwrotnie.
26. Gromadzenie informacji o wystąpieniu zdarzeń operacyjnych (baza zdarzeń).
27. Możliwość generowania ankiet sporządzania na ich podstawie ich wyników raportów.

II. Wymagania międzyobszarowe

1. System powinien posiadać Moduł zarządczy w postaci definiowalnych kokpitów menadżerskich.
2. System musi umożliwiać podpisywanie dokumentów generowanych w Systemie kwalifikowalnym podpisem elektronicznym.
3. Dostawca systemu musi zagwarantować jego aktualizację w przypadku zmian przepisów zewnętrznych, regulacji wewnętrznych i rekomendacji w zakresie zarządzania ryzykiem operacyjnym.
4. System musi umożliwiać archiwizację dokumentów z danego okresu oraz ich przywracanie do bieżącego widoku.

III. Wymagania techniczne

1. Zarządzanie użytkownikami, grupami i prawami dostępu do modułów i funkcji systemu musi być w jednym miejscu w Systemie.