

***Długo oczekiwana norma zarządzania ryzykiem ISO/IEC 27005 została opublikowana w połowie czerwca 2008 roku w ramach serii norm zarządzania ryzykiem ISO/IEC 2700x. Dzięki niej, abstrakcyjne zagadnienie zarządzania ryzykiem (RM) staje się bardziej konkretne dla początkujących i łatwiejsze do wdrożenia nawet w małych i średnich przedsiębiorstwach. Z kolei ze względu na swoją***



***rozbudowaną strukturę i treść, a także szczegółową listę kontrolną, służącą jako skuteczne narzędzie samooceny, jest dla profesjonalistów przewodnikiem do certyfikacji. Dzięki licznym przykładom praktycznym zachęca użytkowników do podążania nowymi drogami lub poszukiwania potwierdzenia prawidłowości swoich działań.***

O ocenę nowego dzieła International Organization for Standardization pytamy w poniższym wywiadzie Herfrieda Geyera, eksperta zarządzania ryzykiem, audytora i trenera jednostki certyfikującej CIS – Certification and Information Security Services.

**W oparciu o jakie treści został rozwinięty standard ISO 27005?**

ISO/IEC 27005 Information Security Risk Management zastępuje TR 13335-3:1998 oraz TR 13335-4:2000, jest zatem rozwinięciem i rozszerzeniem tych raportów technicznych. ISO 27005 dostarcza wytycznych, schematów oraz przykładów zarządzania ryzykiem BI w organizacji, szczególnie w odniesieniu do wymagań ISO 27001 dla bezpieczeństwa informacji.

**Czym jest RM w kontekście działalności gospodarczej?**

Firmy są w pierwszej kolejności zainteresowane dobrymi wynikami biznesowymi, ale nie ochroną danych. To wymaga zaawansowanego IT i dostępności zasobów. Wiąże się to ze stałym zarządzaniem ryzykiem, którego ISO 27001 bezwzględnie wymaga. Kolejne rozszerzanie tej tematyki jest kwestią czasu, kiedy w połowie 2009 roku ukaże się standard zarządzania ryzykiem w przedsiębiorstwach ISO 31000. Całość stanie się nowym tematem dla oficerów bezpieczeństwa, RM w kontekście informacji i jego pomyślne wdrożenie

może odegrać pionierską rolę w zarządzaniu firmą. Menadżerowie jakości i bezpieczeństwa informacji będą w ten sposób rozwijać system zarządzania w sposób zintegrowany.

**Jak ISO 27005 i ISO 31000 mają się do siebie w odniesieniu do zarządzania ryzykiem w firmie?**

ISO 27005 ma podobną konstrukcję i zawiera pokrywające się wytyczne służące integracji RM, ale równie dobrze może być wdrażane samodzielnie. ISO 27005 jest standardem na tyle obszernym, że ISO 31000 nie jest już wymagane jako uzupełnienie RM w sektorze IT. Oba standardy zarządzania ryzykiem podążają w kierunku systemowego podejścia zawartego w modelu doskonalenia procesów Plan-Do-Check-Act i nie podlegają certyfikacji.

**Jakie są powiązania pomiędzy standardami ISO 27005 i ISO 27001?**

Podczas gdy standard ISO 27001 jako wytyczne dla bezpieczeństwa informacji określa co jest do osiągnięcia, ISO 27005 opisuje jak to zrobić. ISO 27005 jest w założeniu pomocnym przewodnikiem, a nie obowiązkowym wymogiem. W wymienionych w załączniku przykładach dotyczących metod szacowania ryzyka podane są modele wstępne, które powinny być dalej dopracowywane i doskonalone. Użytkownik nie powinien trzymać się zbyt blisko istniejących schematów, ale projektować przestrzeń pod kątem korzyści i celów firmy.

**Co możemy znaleźć w nowym RM-ISO 27005?**

Imponujący jest szczegółowy załącznik, zajmujący ponad połowę z około 60 stronicowego dokumentu. Dzięki temu ISO 27005 jest bardzo praktyczny, zawiera wiele przykładów i szczegółowych uwag. Główna część standardu zaczyna się od przeglądu "bezpieczeństwa informacji w procesie zarządzania ryzykiem", dalej są wymienione podstawowe kryteria, szczegóły dotyczące działalności i organizacji. Zorganizowane w przejrzysty sposób staną się elementami zarządzania ryzykiem określanymi przez: szacowanie ryzyka, postępowanie z ryzykiem, zaakceptowanie ryzyka, komunikację ryzyka, monitorowanie i przegląd ryzyka – każde z listą kontrolną i szczegółowymi wyjaśnieniami.

**Czy standard opisuje też metodykę RM?**

To sytuacja na pierwszy rzut oka paradoksalna: z jednej strony ISO 27005 w swojej głównej części nie zawiera metod, ale pewna ich ilość jest dołączona. Są

to jedynie ułatwiające zrozumienie przykłady, w żadnym wypadku nieobowiązkowe.

**Jeden z rozdziałów ISO 27005 koncentruje się na możliwych trudnościach RM bez podawania rozwiązań – jak sobie z tym radzić?**

Postrzegam to jako zachętę do poszukiwania nowych rozwiązań: jak skutecznie zarządzać ryzykiem, pomimo barier kulturowych, religijnych czy społecznych? Jeżeli na przykład niektóre z zadań nie są wykonywane ze względu na wymagający rodzaj pracy, kierownictwo staje przed wyzwaniem minimalizowania ryzyka, zaakceptowania lub jasnego zdefiniowania - włączając mierzalne rezultaty i plany awaryjne. Firma odpowiada za trudności, propagując myślenie otwarte kulturowo: zamiast zaprzeczania problemom, otwarcie się je wyjaśnia. Odważ się - zidentyfikuj problemy i rozwiąż je.

**Czy ISO 27005 może być wdrożone w każdej firmie niezależnie od jej wielkości – także w małym i średnim przedsiębiorstwie?**

Tak, standard jest skalowalny, elastyczny i dlatego niezależny od wielkości czy przedmiotu działalności firmy. Mam nadzieję, że małych i średnich firm nie odstraszy stopień szczegółowości i zakres ISO 27005, ponieważ dzięki wykorzystaniu zwięzłej listy wymagań dla każdego rozdziału, przedsiębiorstwo może łatwo zorientować się, które punkty mogą być stosowane, a które nie. Wychodząc naprzeciw potrzebom przedsiębiorstw, ISO 27005 jest efektywnym ustanowieniem zarządzania ryzykiem, również dla małych i średnich firm.

**Jakie są wady i zalety stosowania ISO 27005?**

Z mojego punktu widzenia, przeważają korzyści, m.in.:

- ISO 27005 jest dobrze skonstruowany
- odniesienia do wymagań ISO 27001 są szczegółowo przytaczane
- załączniki z przykładami i plany szczegółowe są pogłębiane
- krok po kroku prowadzi przez tematykę zarządzania ryzykiem, na „średnim” poziomie zaawansowania, bez specjalistycznej metodologii, niektóre punkty są opisane bardziej szczegółowo w załączniku (ocena aktywów)
- jest bardziej szczegółowy, idee są jasno określone (E2 strona 48)
- koncepcja klasyfikowania informacji

- zalecenia zachęcają do rozpoczęcia analizy szczegółów ryzyka.
- wymagania dla systemu RM są oceniane przez niego samego (rozdział 12).
- rozwiązania nie są podane na tacy ale przez pewnego rodzaju korytarz
- można korzystać z narzędzi oceny, jakkolwiek inne narzędzia i metody niż te wymieniane w ISO 27005 mogą dać także dobre rezultaty w trakcie ustanawiania ISO 27001.

Jako wady mogę wymienić:

- pojęcie "Context" jest nową koncepcją, która w ISO 27001 nie występuje; jak wynika z opisu zawartego w ISO 27005, niektóre wymagania ISO 27001 są bardziej istotne
- wraz z ogromną ilością przykładów i źródeł, istnieje niebezpieczeństwo, zbytniego skupienia się na nich i zapominania o lepszych sposobach; stosując się jedynie do zalecanych przykładów wdrażania ISO 27005 może nie być wystarczające
- zbyt uproszczona definicja ryzyka sprowadzona do prawdopodobieństwa straty czasu
- wymienia się ograniczenia i trudności w implementacji RM, ale nie proponuje się rozwiązań
- przedstawione związki pomiędzy planami i kryteriami akceptacji ryzyka nie są jasno wytłumaczone
- standard rozpoczyna się pytaniem: jak głęboki i szczegółowy może być stopień wdrażania RM .

**Dziękuję za rozmowę.**

