

# ZMIANY W NOWYM WYDANIU NORMY ISO/IEC 27001:2022-10



## BEZPIECZEŃSTWO INFORMACJI, CYBERBEZPIECZEŃSTWO I OCHRONA PRYWATNOŚCI



**MGR INŻ. MICHAŁ MARCZUK**

Główny Specjalista ds. Certyfikacji Systemów Zarządzania  
Departament Certyfikacji i Oceny Zgodności  
Urząd Dozoru Technicznego

Ludzkość żyje w świecie pełnym informacji. Obok wiedzy uchodzą one za podstawowe źródło rozwoju m.in. społecznego, gospodarczego, technicznego. W XXI wieku informacje są niezwykle istotnym zasobem praktycznie każdej organizacji. Mogą one wpływać na jej rozwój, lecz także przy nieodpowiednim podejściu spowodować poważne uszczerbki w funkcjonowaniu firmy, a nawet doprowadzić do jej upadku.

**Bezpieczeństwo w przemyśle petrochemicznym stanowiącym kluczowy sektor gospodarki odgrywa znaczącą rolę. Charakter procesów chemicznych oraz obecność substancji chemicznych w instalacjach wymaga aby zachowano aspekty bezpieczeństwa fizycznego jak również teleinformatycznego.**

Zarządzanie bezpieczeństwem informacji pozwala na bezpieczne działania poprzez wprowadzanie zabezpieczeń, które identyfikują zagrożenia i stawiają im bariery. Międzynarodowym standardem w zarządzaniu bezpieczeństwem informacji jest norma ISO/IEC 27001.

### **NORMA ISO/IEC 27001**

Dokument określa ramy postępowania w dostępie do wszelkich danych istotnych dla organizacji, a więc minimalizuje prawdopodobieństwo, że niepowołana osoba lub instytucja uzyska do nich dostęp w sposób nielegalny lub bez zezwolenia.

Oczywiście wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji nie jest stuprocentową ochroną, niewątpliwie zwiększa bezpieczeństwo organizacji i jej klientów, poprawia jakość procesów bezpieczeństwa oraz zwiększa świadomość pracujących w niej ludzi. Ciągłe zmiany na świecie oraz chęć popularyzacji systemu zarządzania bezpieczeństwem informacji powodują, że toczą się nieustanne prace nad nowymi wersjami normy.

### Najnowszym wydaniem jest wersja ISO/IEC 27001:2022-10 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności.

Formalnie została ona zatwierdzona 23 września 2022 r., natomiast publikacja standardu przypada na 25 października 2022 r. Niedawne wydanie standardu powoduje, że począwszy od 31 października 2022 r., organizacje z wdrożonym SZBI, które oparły swój system na poprzednim wydaniu, są niejako w okresie przejściowym.

Certyfikaty, które zostały wydane zgodnie z normą ISO/IEC 27001:2017, tracą ważność z dniem 31 października 2025 r. Do tego czasu organizacje, które mają wdrożony SZBI według ISO/IEC 27001:2017, powinny przygotować się do audytu przejścia na nowe wydanie normy. Można tego dokonać np. podczas audytu nadzoru, jako oddzielny audyt lub podczas ponownej certyfikacji.

## GŁÓWNE ZMIANY W NORMIE

Co się zatem zmieniło? Ogólna struktura normy pozostała bez zmian. Dokument nadal składa się z dwóch części, tekstu, Normy oraz Załącznika A zawierającego listę zabezpieczeń.

W strukturze normy, tak jak w wydaniu z 2017 r., wyszczególniono 10 punktów odnoszących się do wymagań. Wymagania dotyczą ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia SZBI w organizacji. Podano również dostosowane do potrzeb organizacji wymagania dotyczące szacowania i postępowania z ryzykiem w bezpieczeństwie informacji. Sformułowania wymagań mają charakter ogólny, który nie narzuca konkretnych rozwiązań i jest możliwy do zastosowania w organizacjach każdego rodzaju lub wielkości. Trzeba jednak zaznaczyć, że nie dopuszcza się pominięcia żadnego z wymagań wymienionych w punktach od 4 do 10 przy założeniu, że organizacja deklaruje zgodność z omawianą Normą Międzynarodową.



**Najważniejszymi zmianami ISO/IEC 27001:2022 w stosunku do poprzedniej wersji są nowe wymagania, które dotyczą ustanowienia kryteriów dla procesów operacyjnych i wdrożenia kontroli procesów.** Nowe wymaganie ma zapewniać, że organizacja określa sposób komunikacji. Pojawił się też jeden nowy punkt 6.3 odnoszący się do Planowania Zmian.

**Analizując punkty normy, napotykamy pierwszą zmianę, którą jest punkt 4.4 System zarządzania bezpieczeństwem informacji.** Nowością w tym punkcie jest to, że organizacja powinna wdrożyć, utrzymywać i ciągle doskonalić SZBI, ale nie tylko w stosunku do procesów odnoszących się do filarów, tzn. poufności, integralności oraz dostępności. Należy też uwzględnić procesy i ich interakcje potrzebne do skutecznego wdrożenia systemu, takie jak np. audyt wewnętrzny czy przeglądy zarządzania.

**Kolejną nowością jest punkt 6.3 Planowanie zmian.** Jest to wymaganie, które zostało dodane jako zupełnie nowe w aktualnej wersji normy. Punkt ten odnosi się do zmian w systemie zarządzania bezpieczeństwem informacji. Jeżeli organizacja uzna za potrzebne wprowadzenie zmian w SZBI, to musi te zmiany przeprowadzać w zaplanowany sposób.

W punkcie 7.4 Komunikacja, wraz z określeniem, co należy przekazać, kiedy, z kim i kto ma się komunikować, istnieje wymóg określenia, w jaki sposób ta komunikacja będzie się odbywać. Określenie sposobu komunikacji jest wymaganiem, które odróżnia aktualną wersję standardu od wersji z 2017 r.

**Biorąc pod uwagę możliwość wycieków toksycznych substancji, awarie czy nawet wypadki, prawidłowo zorganizowana forma komunikacji jest istotnym zabezpieczeniem dla realizacji procedur awaryjnych. Dobrze określone i utrzymywane sposoby komunikacji zapewniają prawidłową współpracę ze służbami lub innymi podmiotami, które mogą pomóc w zniwelowaniu skutków ewentualnego zakłócenia.**

**Dużo większe zmiany zaszły w Załączniku A, którego struktura została całkowicie zmieniona.** Zrezygnowano ze 114 zabezpieczeń podzielonych na 14 sekcji na rzecz 93 zabezpieczeń pogrupowanych w 4 sekcjach. Taki układ załącznika jest bardziej przejrzysty i agreguje zabezpieczenia tematycznie. Punkt A5 „Organizacyjne zabezpieczenia” zawiera 37 zabezpieczeń, z czego 3 są nowe. Punkt A6 „Osobowe zabezpieczenia” pozostaje praktycznie bez zmian i zawiera 8 zabezpieczeń. Punkt A7 „Fizyczne zabezpieczenia” to zbiór 14 zabezpieczeń, w tym jedno nowe, oraz punkt 8 „Technologiczne zabezpieczenia” to zestaw 34 zabezpieczeń i w tej części otrzymujemy 7 nowych.

Aktualizacja wymagań wynika z konieczności odniesienia do najnowszych i najlepszych praktyk oraz rezygnacji z przestarzałych technologii na rzecz nowych. Przechodząc do analizy zabezpieczeń, na poziomie organizacyjnym, wprowadzono w punkcie 5.7 zabezpieczenie dotyczące analizy zagrożeń. Należy zatem identyfikować zagrożenia wewnętrzne i zewnętrzne, które mogą mieć wpływ na funkcjonowanie organizacji. Jakiego rodzaju metody i narzędzia może wykorzystywać osoba atakująca, skąd można czerpać wiedzę na temat tych ataków, kto powinien gromadzić informacje pomocne przy przeciwdziałaniu oraz kto powinien je analizować. Wymaganie to nakłada na organizację wymóg wyznaczenia osoby lub zespołu, który będzie za takie działania odpowiedzialny.

Technologie chmurowe są w środowisku IT już bardzo rozpowszechnione. Umożliwiają one przetwarzanie informacji przy pomocy zasobów obliczeniowych poprzez sieć internet. Technologia ta daje ogromne możliwości, ale niesie ze sobą również wiele zagrożeń. Norma ISO/IEC 27001:2022 w odróżnieniu od poprzedniej edycji wychodzi naprzeciw tym zagrożeniom. **W punkcie A5.23 Załącznika A dodano zabezpieczenie „Bezpieczeństwo informacji do użytku w usługach w chmurze”.** Zapis ten odnosi się całościowego zarządzania procesami związanymi z usługami chmurowymi, co oznacza, że bezpieczeństwo informacji powinno być brane pod uwagę na każdym etapie. Zaczynając od wyboru usługodawcy, poprzez określenie wymagań umownych oraz obowiązków dostawcy usług, kończąc na zachowaniu bezpieczeństwa informacji w trakcie trwania umowy oraz po jej zakończeniu.

**Ostatnim nowym zabezpieczeniem dodanym w części organizacyjnej jest punkt A5.30 „Gotowość teleinformatyczna do zapewnienia ciągłości działania”.** Jest to odniesienie wprost do normy ISO IEC 22301 System Zarządzania Ciągłością Działania w kontekście systemów teleinformatycznych. Oznacza to, że kadra zarządzająca tymi systemami powinna określić w wyniku analizy BIA (Business Impact Analysis) systemy krytyczne do zapewnienia funkcjonowania organizacji. W ramach tej analizy należy też odnieść się do pojęć bezpośrednio wywodzących się z ciągłości działania – wyznaczenie punktów:

- RPO (Recovery Point Objective), czyli poziomu, do którego organizacja może pozwolić sobie na utratę danych,
- RTO (Recovery Time Objective), czyli okresu następującego po incydencie, w którym produkt i usługa lub działanie są wznawiane, a zasoby są odzyskiwane.

Poziomy tych czynników są wprost zależne od krytyczności danego systemu ICT.

## ROLA BEZPIECZEŃSTWA INFORMACJI

Zapewnienie bezpieczeństwa informacji nie opiera się jedynie na zabezpieczeniu technologii informatycznych. Bezpieczeństwo fizyczne jest równie istotne. Brak zabezpieczeń w tym zakresie może doprowadzić do nieupoważnionego dostępu do informacji istotnych dla organizacji.

**Niepowołane osoby poruszające się po obiekcie przemysłowym mogą stanowić zagrożenie dla siebie oraz infrastruktury. Próby podłączenia zewnętrznych urządzeń lub zmiany ustawień już istniejących mogą niekorzystnie wpływać na przetwarzane procesy stanowiące podstawę działania organizacji.**

**Nowym zabezpieczeniem wprowadzonym w normie ISO/IEC 27001:2022 jest w punkcie A7.4 „Monitorowanie bezpieczeństwa fizycznego”.** Innymi słowy, należy prowadzić nadzór nad przepisami i regulacjami dotyczącymi ochrony danych w połączeniu z nadzorem wszelkich systemów ochrony fizycznej, takich jak np. systemy CCTV, RFID, detektory ruchu, czujniki ogrodzeniowe. Stały nadzór nad nimi ogranicza możliwość wystąpienia wyżej wymienionych zagrożeń.

**Najbardziej rozbudowanym jest punkt A8 stanowiący listę zabezpieczeń odnoszących się do użytej technologii informacyjnej.**

Pierwszym z nowych punktów jest A8.9 „Zarządzanie konfiguracją”. Istotą tego zabezpieczenia jest systemowe podejście do nadzoru nad systemami lub sprzętem komputerowym, który jest używany do przetwarzania informacji. Nieautoryzowane zmiany w ich konfiguracji mogą doprowadzić do niekontrolowanej eksploracji lub zmiany danych przez nieupoważnione osoby. Należy więc wdrożyć narzędzia, które pozwolą przede wszystkim na wymuszenie zdefiniowanych konfiguracji sprzętu czy oprogramowania, ale również na dalsze monitorowanie pod kątem zmian.

Punkt A8.10 „Usuwanie informacji” reguluje kwestię przechowywania informacji na urządzeniach lub mediach. Informacje, które nie są używane czy potrzebne,

powinny zostać usunięte, żeby zapobiec niepożądanym wyciekom. Decyzja o tym, jakie dane mają zostać usunięte i w jaki sposób, powinna być zgodna z przepisami prawa, ale również z wewnętrznymi regulacjami organizacji – zgodnie z klasyfikacją informacji, która została przyjęta. Zabezpieczenie to ma zastosowanie nie tylko w przypadku nośników danych, takich jak np. dyski twarde czy urządzenia. Norma zakłada, że organizacja podejmie też stosowne kroki w tym zakresie w relacjach z dostawcami. Należy wdrożyć mechanizmy, które zapewnią, że w przypadku rozwiązania umowy z dostawcą rozwiązań chmurowych wrażliwe dane należące do organizacji także zostaną usunięte.

Usunięcie zbędnych informacji jest jednym ze sposobów na zapewnienie, że nie dostaną się w niepowołane ręce. A jeśli organizacja ich nadal potrzebuje?

**Zabezpieczeniem regulującym tę kwestię może być punkt A8.11 „Maskowanie danych”.** Działanie prewencyjne, jakim jest maskowanie danych, ma na celu ograniczenie ekspozycji informacji w zależności od ich kontekstu. Mogą to być informacje istotne z punktu widzenia biznesu, danych osobowych, ale także relacyjnych w odniesieniu do struktur bazodanowych. W związku z powyższym, tak jak w przypadku usuwania danych, techniki, jakie zostaną użyte do maskowania, powinny być zgodne ze zobowiązaniami prawnymi, regulacyjnymi oraz umownymi.

**Działania prewencyjne, bo taki charakter mają dwa powyższe zabezpieczenia, w logiczny sposób wspomagają działania organizacji do zabezpieczenia A8.12 Zapobieganie wyciekom danych.** Oczywiście, tak samo jak w poprzednich przypadkach, podstawą do podjęcia decyzji o krytyczności informacji jest ich identyfikacja oraz klasyfikacja. Kanały, którymi informacja może wycieć, są różne. Niezabezpieczone urządzenia lub systemy komputerowe, które przetwarzają informacje, nie są jedynym źródłem wycieku. Często powodem wycieku, świadomego lub nie, są ludzie. Dlatego też poza wdrożeniem systemów DLP, skutecznym sposobem na zapobieganie wyciekom jest edukacja personelu.

**Obydwu zagrożeniom, jakimi są technologia i ludzie, odpowiadają dwa kolejne zabezpieczenia. Są to punkty A8.16 „Działania monitorujące” oraz A8.23 „Filtrowanie sieci”.** Z technicznego punktu widzenia wymagania te stanowią o konieczności działań operacyjnych skierowanych na zabezpieczenie przed złośliwym oprogramowaniem, monitorowanie systemów sieciowych i aplikacji pod kątem nietypowych zachowań czy zdolności do przystosowania się do różnych zagrożeń. Stosowanie narzędzi typu IPS, IDS, Firewalli czy systemów DLP pomaga administratorom w proaktywnym kontrolowaniu środowiska teleinformatycznego.

Z drugiej strony ustanowienie zasad bezpiecznego i odpowiedniego korzystania z zasobów internetowych czy identyfikacja typów stron internetowych jest narzędziem skierowanym do użytkowników. Regulacje w tym zakresie wraz z zapewnieniem odpowiednich szkoleń zmniejszają możliwość wykonania przez użytkowników działań niepożądanych.

W dzisiejszych czasach chyba nie ma organizacji, która by nie korzystała z różnego rodzaju oprogramowania. Należy więc przyjąć, że aplikacja jest tylko wtedy dobrze zaprojektowana i napisana, kiedy założeniem przy jej budowie będzie to, że jest potencjalnym punktem ataku. **Ostatnie z nowych zabezpieczeń w normie ISO/IEC 27001:2022 odnosi się do środowiska deweloperskiego. W punkcie A8.28 „Bezpieczne kodowanie” norma wymaga, aby organizacja określiła procesy, które zapewnią nadzór nad całym cyklem życia tworzonych aplikacji.** Należy więc wdrożyć zabezpieczenia już na etapie projektowania, zapewnić szkolenia dla programistów, tak aby stosowali najlepsze praktyki w tym zakresie, a także zapewnić bezpieczne środowisko deweloperskie. Stworzone oprogramowanie należy testować pod kątem bezpieczeństwa informacji zgodnie z dostępną wiedzą o rzeczywistych zagrożeniach. Pełny zestaw wytycznych do wdrożenia tego zabezpieczenia można odnaleźć w normie PN-EN ISO/IEC 27002:2022.

## WYZWANIA BEZPIECZEŃSTWA

Zmiany zachodzące we współczesnym świecie w naturalny sposób wymusiły potrzebę aktualizacji normy ISO/IEC 27001. Rozszerzone o czynniki zewnętrzne środowisko funkcjonowania, zapewnienie ciągłości działania czy uwzględnienie nowoczesnej technologii to czynniki wpływające na pogłębianie się dojrzałości branży cyberbezpieczeństwa. Nowe wydanie standardu stara się więc odpowiadać na wyzwania bezpieczeństwa informacji stawiane przed organizacjami.