Najważniejsze zmiany w ISO/IEC 27002:2022

BIAŁA KSIEGA

Wprowadzenie

ISO/IEC 27002 jest dokumentem zawierającym wytyczne i ma służyć jako punkt odniesienia przy wyborze zabezpieczeń podczas wdrażania Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w oparciu o ISO/IEC 27001 lub jako przewodnik dla organizacji wdrażających powszechnie akceptowane zabezpieczenia bezpieczeństwa informacji. Poprzednia edycja ISO/IEC 27002:2013 była poddawana przeglądowi od 2018 r przez ISO/IEC JTC 1/SC27, a nowe wydanie zostało oficjalnie opublikowane 15 lutego 2022 r.

Chociaż część elementów sterujących pozostaje niezmieniona, istnieją znaczące zmiany w układzie elementów sterujących i innych zabezpieczeniach. Ponieważ załącznik A z normy ISO/IEC 27001:2013 musiał zostać dostosowany do normy ISO/IEC 27002, norma ISO/IEC 27001:2013 została także poddana rewizji i jej zaktualizowana wersja została opublikowana w październiku 2022 r.

W tym artykule zwrócono uwagę na kluczowe zmiany w ISO/IEC 27002:2022 r. w porównaniu z wydaniem z 2013 r.

Kluczowe zmiany

Liczba zabezpieczeń | 93

W edycji 2022 jest 93 zabezpieczeń w porównaniu z 114 zabezpieczeniami w edycji 2013.

Kategorie zabezpieczeń | 4

Zabezpieczenia zostały przegrupowane w 4 kategorie, zamiast 14 tematów i 35 kategorii w edycji 2013.

Układ czterech kategorii podkreśla, że ochrona informacji i danych to coś więcej niż tylko środki technologiczne. Zabezpieczenia technologiczne to tylko środki zaradcze zapobiegające zagrożeniom związanym z bezpieczeństwem informacji lub je łagodzące i nie wystarczą do osiągnięcia wyników w zakresie bezpieczeństwa informacji.

Co ważniejsze, najwyższe kierownictwo organizacji musi określić ramy i kierunek zarządzania bezpieczeństwem informacji, a także zidentyfikować i przekazać znaczenie i wpływ różnych informacji na biznes i organizację.

Poza tym ten nowy układ zabezpieczeń może ułatwić kierownictwu przypisanie obowiązków w ramach organizacji w celu zwiększenia bezpieczeństwa informacji.

ISO/IEC 27002:2022	
5	Zabezpieczenia organizacyjne
6	Zabezpieczenia dotyczące ludzi
7	Zabezpieczenia fizyczne
8	Zabezpieczenia technologiczne

ISO/IEC 27002:2013		
5 Polityki bezpieczeństwa informacji	6 Organizacja bezpieczeństwa informacji	7 Bezpieczeństwo zasobów ludzkich
8 Zarządzanie aktywami	9 Kontrola dostępu	10 Kryptografia
11 Bezpieczeństwo fizyczne i środowiskowe	12 Bezpieczna eksploatacja	13 Bezpieczeństwo komunikacji
14 Pozyskiwanie, rozwój i utrzymanie systemów	15 Relacje z dostawcami	16 Zarządzanie incydentami związanymi z bezpieczeństwem informacji
17 Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania		18 Zgodność

* Każda norma ISO podlega przeglądowi co pięć lat. Począwszy od marca 2018 r. ISO JTC1/SC27 zaproponował aktualizację standardu, biorąc pod uwagę rozwój nowych technologii, pojawiające się zagrożenia i zmieniające się praktyki przemysłowe.

Nowe Zabezpieczenia | 11

Wprowadzono 11 nowych zabezpieczeń aby uwzględnić rozwój technologii i praktyk przemysłowych.

5.7	Analiza zagrożeń	Organizacje powinny zachować czujność i świadomość stale zmieniającego się środowiska zagrożeń. Istnieją różne poziomy analizy zagrożeń: strategiczny, taktyczny i operacyjny. Informacje o zagrożeniach taktycznych i operacyjnych mogą pochodzić z wniosków wyciąganych od różnych zespołów roboczych (zabezpieczenie 5.6 Kontakt z zespołami roboczymi), wniosków wyciągniętych z incydentów związanych z bezpieczeństwem informacji (zabezpieczenie 5.27 Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji) lub Centrum Operacji Bezpieczeństwa (SOC). Tymczasem organizacje powinny dostrzegać zmieniający się krajobraz zagrożeń, nie tylko w swojej branży, ale także w innych branżach.
5.23	Bezpieczeństwo informacji przy korzystaniu z usług w chmurze	Nie ulega wątpliwości, że dodanie tego nowego zabezpieczenia ma być odpowiedzią na coraz częstsze korzystanie z usług chmurowych przez organizacje w trakcie ostatniej dekady. Chociaż jest to zabezpieczenie organizacyjne, właściwe korzystanie z tego zabezpieczenia wymaga wiedzy technicznej na temat technologii związanych z rozwiązaniami chmurowymi. W związku z tym organizacje mogą rozważyć zaangażowanie ekspertów od rozwiązań chmurowych podczas wdrażania tego zabezpieczenia.
5.30	Gotowość teleinformatyczna do zapewnienia ciągłości biznesowej	Cel tego nowego zabezpieczenia różni się od zabezpieczenia 5.29 (Bezpieczeństwo informacji podczas zakłóceń). Ma na celu zapewnienie dostępności informacji organizacji i innych powiązanych zasobów podczas zakłóceń. Przykładem wdrożenia tego zabezpieczenia może być opracowany przez dział IT plan odzyskiwania po awarii (DRP), pod warunkiem, że uwzględnia on wymagania organizacji dotyczące ciągłości działania. Zabezpieczenie 5.29 (Bezpieczeństwo informacji podczas zakłóceń) ma na celu utrzymanie poufności, integralności i dostępności informacji podczas zakłóceń, np. kontrola dostępu fizycznego jest tymczasowo niedostępna z powodu zawieszenia zasilania.
7.4	Monitorowanie bezpieczeństwa fizycznego	Chociaż jest to nowe zabezpieczenie zgodnie z Załącznikiem B do normy ISO/IEC 27002:2022, wiele organizacji powinno już ją wdrożyć w swoich obiektach, np. instalując system nadzoru, system wykrywania włamań lub system kontroli dostępu do drzwi itp.
8.9	Zarządzanie konfiguracją	Zarządzanie konfiguracją powinno być aktywnym procesem zarządzania konfiguracjami sprzętu, oprogramowania, usług (np. usług w chmurze) i sieci w całym ich cyklu życia. Przykładem implementacji tego zabezpieczenia jest utwardzanie systemu. Konfiguracje należy zachować, aby zapewnić ich skuteczność. Zmiany powinny być przeprowadzane w kontrolowany sposób, zgodnie z procesem zarządzania zmianami 8.32 (Zarządzanie zmianami), a zapisy zmian powinny być bezpiecznie przechowywane.
8.10	Usuwanie informacji	Dodanie tych trzech zabezpieczeń nawiązuje do tytułu wydania z 2022 r. (Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Zabezpieczenia bezpieczeństwa informacji). Zabezpieczenia te są powszechnie przyjęte w obowiązujących przepisach dotyczących prywatności danych i normach międzynarodowych, np. GDPR (RODO), ISO/IEC 27701, w celu ochrony praw osób, których dane dotyczą.
8.11	Maskowanie danych	
8.12	Zapobieganie wyciekom danych	
8.16	Działania monitorujące	To nowe zabezpieczenie ma na celu monitorowanie sieci, systemów i aplikacji pod kątem nietypowych zachowań i potencjalnych incydentów związanych z bezpieczeństwem informacji. Organizacje przyjęły różne środki monitorowania, aby monitorować swoje środowisko IT, np. instalując oprogramowanie antywirusowe, zapory sieciowe lub filtry sieciowe z logowaniem.
8.23	Filtrowanie sieci	To nowe zabezpieczenie jest stosunkowo proste. Wiele organizacji wdrożyło je w swojej sieci IT. Im więcej zewnętrznych witryn internetowych jest monitorowanych, tym mniejsze jest narażenie organizacji na szkodliwą zawartość tych stron. Organizacje powinny zrównoważyć ryzyko związane z bezpieczeństwem informacji i potrzeby biznesowe.
8.28	Bezpieczne kodowanie	To nowe zabezpieczenie ma na celu zmniejszenie liczby potencjalnych luk w zabezpieczeniach w nowo tworzonym lub udoskonalonym oprogramowaniu. W wydaniu z 2013 roku pominięto to zabezpieczenie.

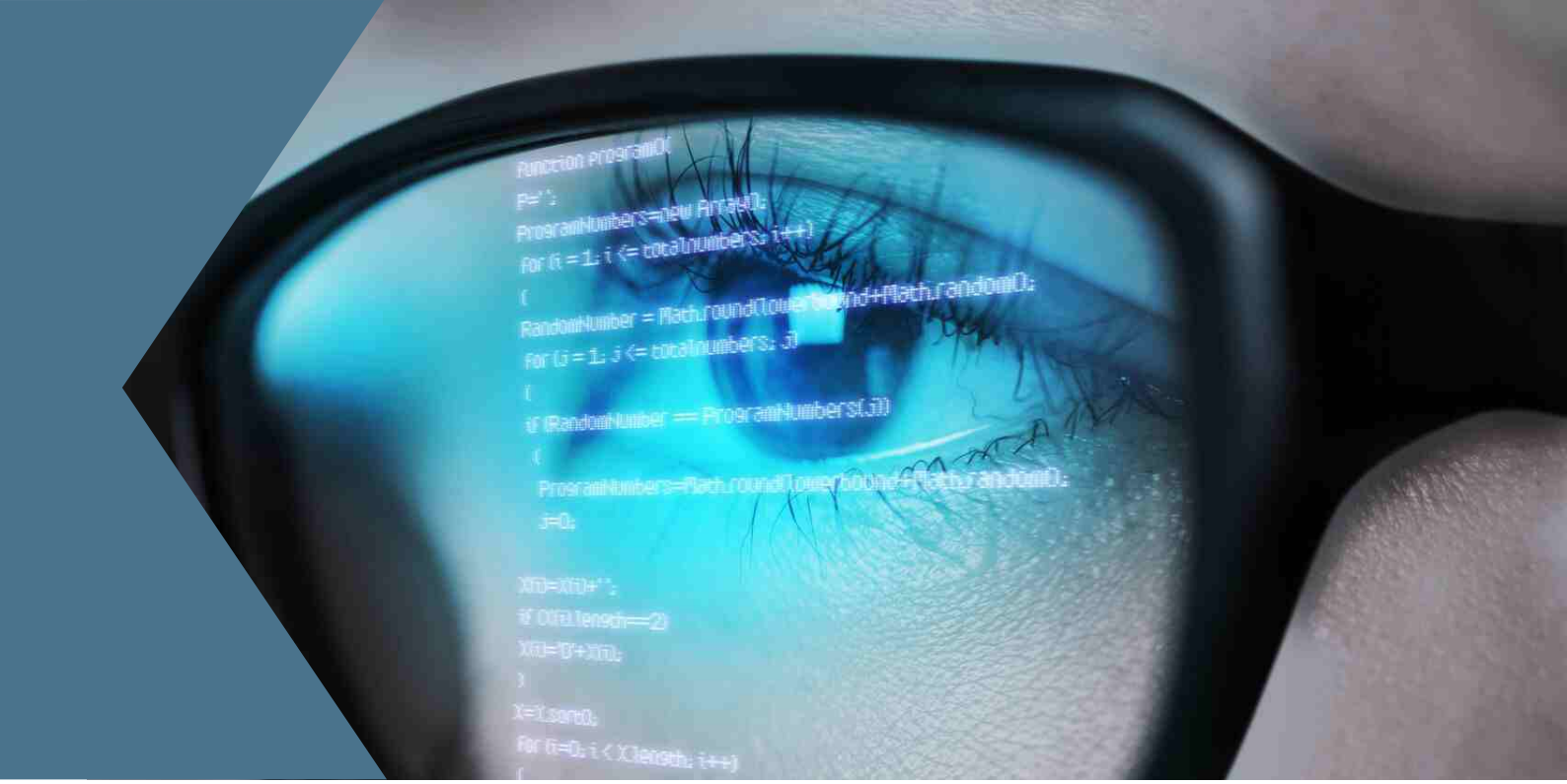
Połączone Zabezpieczenia | 24

24 zabezpieczenia w edycji 2022 są wynikiem połączenia niektórych zabezpieczeń z edycji 2013. Łączenie zabezpieczeń skutkuje zmniejszeniem ich liczby, a tym samym tworzeniem szczuplejszego standardu.

Uwaga: Część scalonych zabezpieczeń została wyodrębniona i pokazana w poniższej tabeli. Odbiorcy mogą zapoznać się z załącznikiem B do normy ISO/IEC 27002:2022, aby zapoznać się z pełną listą połączonych zabezpieczeń.

ISO/IEC 27002:2022		ISO/IEC 27002:2013		UWAGA
Zabezpieczenia, które są nierozłączne we wdrażaniu, zostają połączone.				
5.1	Polityki bezpieczeństwa informacji	5.1.1	Polityka bezpieczeństwa informacji	Przegląd polityk bezpieczeństwa informacji nie jest możliwy w przypadku braku takich polityk. Podczas gdy zasady powinny być regularnie przeglądane, aby były aktualne.
		5.1.2	Przegląd polityk bezpieczeństwa informacji	
5.9	Spis informacji i innych powiązanych aktywów	8.1.1	Inwentaryzacja majątku	Identyfikacja własności aktywów nie jest możliwa, jeśli nie zidentyfikowano żadnych aktywów. Należy opracować i utrzymywać wykaz aktywów, w tym także ich właścicieli, aby zapewnić właściwe zarządzanie i ochronę tych aktywów.
		8.1.2	Własność aktywów	
5.10	Akceptowalne wykorzystanie informacji i innych powiązanych aktywów	8.1.3	Akceptowalne użycie aktywów	Korzystanie z aktywów z pewnością obejmuje obchodzenie się z aktywami.
		8.2.3	Postępowanie z aktywami	
8.24	Użycie kryptografii	10.1.1	Polityka stosowania zabezpieczeń kryptograficznych	Zarządzanie kluczami nie jest możliwe, jeśli nie są używane zabezpieczenia kryptograficzne, np. szyfrowanie. Ochrona informacji za pomocą szyfrowania jest bezużyteczna, jeśli klucz nie jest odpowiednio chroniony.
		10.1.2	Zarządzanie kluczami	
Niektóre zabezpieczenia są scalane z rozszerzeniem zakresu.				
5.8	Bezpieczeństwo informacji w zarządzaniu projektami	6.1.5	Bezpieczeństwo informacji w zarządzaniu projektami	Połączone zabezpieczenia mają na celu nie tylko ograniczenie zagrożeń dla bezpieczeństwa informacji związanych z projektami, ale także rezultatów projektu, np. nowo opracowanego oprogramowania.
		14.1.1	Analiza i specyfikacja wymagań związanych z bezpieczeństwem informacji	
8.1	Urządzenia końcowe użytkownika	6.2.1	Polityka stosowania urządzeń mobilnych	Prawie wszystkie urządzenia mobilne to urządzenia użytkowników końcowych. Jednak stacja robocza jest urządzeniem końcowym użytkownika, ale nie jest urządzeniem mobilnym. Organizacje, które ustanowiły politykę dotyczącą urządzeń mobilnych zgodnie z ISO/IEC 27002:2013, powinny dokonać przeglądu zakresu polityki i zaktualizować ją, aby obejmowała wszystkie używane urządzenia końcowe użytkowników.
		11.2.8	Pozostawianie sprzętu użytkownika bez opieki	

8.26	Wymagania bezpieczeństwa aplikacji	14.1.2	Zabezpieczanie usług aplikacyjnych w sieciach publicznych	Powstałe z połączenia zabezpieczenie ma na celu na celu nie tylko ograniczenie zagrożeń dla bezpieczeństwa informacji związanych z usługami aplikacyjnymi w sieciach publicznych, np. handlem elektronicznym i transakcjami, ale także zapobieganie zagrożeniom dla bezpieczeństwa informacji we wszystkich rodzajach aplikacji i usług aplikacyjnych.
		14.1.3	Ochrona transakcji usług aplikacji	
Podobne zabezpieczenia są zharmonizowane, aby stały się jednym zabezpieczeniem.				
5.14	Przesyłanie informacji	13.2.1	Polityki i procedury przesyłania informacji	• Niektóre zabezpieczenia w wydaniu z 2013 r. są ukryte w szczegółowych wskazówkach w wydaniu z 2022 r. po połączeniu. Większość wchłoniętych zabezpieczeń pozostaje jednak istotna dla zapobiegania zagrożeniom bezpieczeństwa informacji i je ogranicza, np. regularny przegląd praw dostępu, regularne testowanie planu ciągłości bezpieczeństwa informacji. Użytkownikom wydania z 2022 r. zaleca się przeczytanie wskazówek dotyczących każdego zabezpieczenia w celu skutecznego wdrożenia. • Chociaż zgodnie z Załącznikiem B do normy ISO/IEC 27002:2022, zabezpieczenie 8.3.3 (Przekazywanie nośników) z wydania z 2013 r. zostało połączone z zabezpieczeniem 7.10 (Nośniki pamięci) w wydaniu z 2022 r., wskazówki dotyczące przekazywania nośników są określone zabezpieczeniem 5.14 (Przesyłanie informacji). • Wszystkie zabezpieczenia związane ze zmianami z edycji 2013 zostały połączone w jedno zabezpieczenie zarządzania zmianami w edycji 2022. To nie jedyna zmiana, także zakres zabezpieczenia 8.32 (Zarządzanie zmianą) został również zawężony do zmian w urządzeniach do przetwarzania informacji i systemach informacyjnych. W przeciwieństwie do innych wchłoniętych zabezpieczeń znaczna część wskazówek dotyczących zabezpieczeń związanych ze zmianami z wydaniz z 2013 r. została usunięta.
		13.2.2	Porozumienia dotyczące przesyłania informacji	
		13.2.3	Wiadomości elektroniczne	
5.17	Informacje uwierzytelniające	9.2.4	Zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników	
		9.3.1	Stosowanie poufnych informacji uwierzytelniających	
		9.4.3	System zarządzania hasłami	
5.18	Prawa dostępu	9.2.2	Przydzielanie dostępu użytkownikom	
		9.2.5	Przegląd praw dostępu użytkowników	
		9.2.6	Odbieranie lub dostosowywanie praw dostępu	
5.29	Bezpieczeństwo informacji podczas zakłóceń	17.1.1	Planowanie ciągłości bezpieczeństwa informacji	
		17.1.2	Wdrażanie ciągłości bezpieczeństwa informacji	
		17.1.3	Weryfikowanie, przegląd i ocena ciągłości bezpieczeństwa informacji	
7.10	Nośniki pamięci	8.3.1	Zarządzanie nośnikami wymiennymi	
		8.3.2	Wycofywanie nośników	
		8.3.3	Przekazywanie nośników	
		11.2.5	Usunięcie aktywów	
8.15	Rejestrowanie zdarzeń	12.4.1	Rejestrowanie zdarzeń	
		12.4.2	Ochrona informacji w dziennikach zdarzeń	
		12.4.3	Rejestrowanie działań administratorów i operatorów	
8.32	Zarządzanie zmianami	12.1.2	Zarządzanie zmianami	
		14.2.2	Procedury kontroli zmian w systemach	
		14.2.3	Przegląd techniczny aplikacji po zmianach w platformie produkcyjnej	
		14.2.4	Ograniczenia dotyczące zmian w pakietach oprogramowania	



Atrybuty

Oprócz nowych zabezpieczeń, edycja 2022 wprowadza „atrybuty" dla każdego zabezpieczenia.
Każde zabezpieczenie jest powiązane z pięcioma atrybutami z odpowiadającymi im wartościami atrybutów.

ATRYBUT	WARTOŚĆ ATRYBUTU	UWAGA
Rodzaje zabezpieczeń	Prewencyjne, wykrywajace, korygujące	Spojrzenie na zabezpieczenie z perspektywy tego, kiedy i w jaki sposób zabezpieczenie modyfikuje ryzyko w związku z wystąpieniem incydentu związanego z bezpieczeństwem informacji.
Właściwości bezpieczeństwa informacji	Poufność, integralność, dostepność	Spojrzenie na zabezpieczenie z punktu widzenia tego, którą cechę informacji zabezpiecza.
Koncepcje cyberbezpieczeństwa	Identyfikuj, chroń, wykrywaj, reaguj i odzyskuj	Spojrzenie na zabezpieczenie z perspektywy powiązania zabezpieczenia z koncepcjami cyberbezpieczeństwa zdefiniowanymi w ISO/IEC TS 27110 i NIST Cybersecurity Framework.
Możliwości operacyjne	Zarządzanie, zarządzanie_zasobami, ochrona_informacji, bezpieczeństwo_zasobów_ludzkich, bezpieczeństwo_fizyczne, bezpieczeństwo_systemu_i_sieci, bezpieczeństwo_aplikacji, bezpieczna_konfiguracja, zarządzanie_identyfikacją_i_dostępem, zarządzanie_zagrożeniami_i_lukami_w_zabezpieczeniach, ciągłość, bezpieczeństwo_relacji_z_dostawcami, zgodność_prawna_i_zgodność, zarządzanie_bezpieczeństwem_informacji, zapewnienie_bezpieczeństwa_informacji	Spojrzenie na zabezpieczenie z perspektywy praktyka w zakresie możliwości związanych z bezpieczeństwem informacji. Istnieje łącznie 15 wartości atrybutów. Większość z nich jest podobna do tematów zabezpieczeń edycji 2013.
Domeny bezpieczeństwa	Zarządzanie_i_ekosystem, ochrona, obrona, odporność	Aby spojrzeć na zabezpieczenie z perspektywy domen bezpieczeństwa informacji, wiedzy specjalistycznej, usług i produktów

Załącznik A do normy ISO/IEC 27002:2022 przedstawia wykorzystanie atrybutów jako sposobu tworzenia różnego podejścia do zabezpieczeń.
Niemniej jednak pewne jest, że stosowanie atrybutów nie jest obowiązkowe. Organizacje mogą zignorować jeden lub więcej atrybutów lub wybrać inne atrybuty, np. model dojrzałości.

„Powód" zastąpił „Cel"

Jak już wspomniano, ISO/IEC 27002: 2013 zawierało 14 tematów i 35 kategorii zabezpieczeń. Dla każdej kategorii bezpieczeństwa definiowało cel zabezpieczenia określający, co ma zostać osiągnięte.
Zawierało jedno lub więcej zabezpieczeń, które można zastosować, aby osiągnąć zamierzony cel zabezpieczenia

W wydaniu z 2022 r. „cel" został zastąpiony „powodem". Poza tym, każde zabezpieczenie ma określony powód jego stosowania, aby zilustrować, dlaczego zabezpieczenie powinno zostać wdrożone.

Inne zmiany

TYTUŁ

Tytuł edycji 2022 został zmieniony na Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Kontrola bezpieczeństwa informacji. Usunięto termin „Kodeks postępowania", aby odzwierciedlić fakt, że dokument odnosi się do ogólnych zabezpieczeń bezpieczeństwa informacji.

TERMINY I DEFINICJE

ISO/IEC 27000 nie jest już odniesieniem normatywnym dla wydania z 2022 r. W zamian, zastosowanie mają terminy i definicje zawarte w punkcie 3 ISO/IEC 27002:2022. Użytkownikom wydania z 2022 r. zaleca się zapoznanie się z terminami i definicjami, aby ułatwić im zrozumienie zabezpieczeń i wskazówek zawartych w dokumencie.

Podsumowanie

Chociaż wyjaśnienie i uzasadnienie zmian w wydaniu z 2022 roku nie zostało opublikowane poza JTC 1/SC27, oczywiste jest, że zmiany mają odzwierciedlać postęp techniczny i ewoluujące praktyki przemysłowe.

Jak wspomniano we wstępie, opublikowana została także poprawiona wersja ISO/IEC 27001:2022.

Dotychczasowa lista zabezpieczeń z Załącznika A w ISO/IEC 27001:2013 została zastąpiona zabezpieczeniami z nowego ISO/IEC 27002:2022. Informacje na temat zmian w ISO/IEC 27001:2022 zawarliśmy w białej księdze: Eskalacja zagrożeń, innowacyjna technologia i lepsza łączność – znaczenie i ewolucja ISO/IEC 27001

WWW.SGS.PL

SGS Polska

pl.certyfikacja@sgs.com

+48 22 329 22 93

www.sgs.pl

www.facebook.com/SGS

www.linkedin.com/company/sgs

WHEN YOU NEED TO BE SURE