Eskalacja zagrożeń, innowacyjna technologia i lepsza łączność – znaczenie i ewolucja ISO/IEC 27001

BIAŁA KSIĘGA

WWW.SGS.PL

SGS

Ewolucja cyberzagrożeń

Razem z rozwojem Przemysłu 4.0 i Internetu Rzeczy (IoT) zagrożenia cybernetyczne stały się bardziej wyrafinowane. Ataki zdarzają się niemalże codziennie i dotyczą nie tylko atakowanego przedsiębiorstwa, ale także jego partnerów biznesowych, dostawców i klientów.

Globalna pandemia i wojna rosyjsko-ukraińska również wpłynęły na znaczący wzrost cyberataków. Konflikt pokazał, że działania wojenne nie ograniczają się tylko do pola bitwy, ale także toczą się w domenie cyfrowej, gdzie sponsorowane przez państwo ugrupowania cyberprzestępcze próbują szerzyć dezinformację i destabilizować infrastrukturę krytyczną.

Organizacje, osoby prywatne i narody muszą nadążać za ewolucją zagrożeń cybernetycznych i wdrażać najnowsze środki ochrony, aby uniknąć między innymi utraty danych, procesów sądowych i utraty reputacji.

Definiowanie zagrożeń

Bezpieczeństwo informacji

Bezpieczeństwo informacji, znane również jako InfoSec, odnosi się do procesów i narzędzi używanych do ochrony poufnych informacji biznesowych przed modyfikacją, zakłóceniem, zniszczeniem czy ujawnieniem.

Cyberbezpieczeństwo

Cyberbezpieczeństwo to praktyka ochrony systemów, sieci i programów przed atakami cyfrowymi. Te cyberataki mają zwykle na celu przejęcie, zmianę lub zniszczenie poufnych informacji, wyłudzenie pieniędzy użytkowników lub zakłócenie normalnych procesów biznesowych.

Ochrona prywatności

Ochrona prywatności zabezpiecza dane osobowe przed dostaniem się w niepowołane ręce, np. hakerów. Sposób określenia może się różnić w zależności od osoby, firmy, jednostki.

10 największych zagrożeń

1. TECHNOLOGIA O NISKIM POZIOMIE ZABEZPIECZEŃ

Technologia rozwija się szybciej niż kiedykolwiek. Najczęściej nowe technologie mają dostęp do Internetu, ale nie mają wdrożonych żadnych mechanizmów zabezpieczających. Stwarza to poważne ryzyko, ponieważ każde niezabezpieczone połączenie oznacza lukę w zabezpieczeniach.

2. ATAKI W MEDIACH SPOŁECZNOŚCIOWYCH

Cyberprzestępcy nieustannie znajdują nowe sposoby wykorzystywania użytkowników mediów społecznościowych i ich prywatnych informacji. Jednym ze złośliwych sposobów jest użycie emotikonek, aby użytkownik stracił czujność.

3. MOBILNE ZŁOŚLIWE OPROGRAMOWANIE (MALWARE)

Eksperci ds. bezpieczeństwa dostrzegli zagrożenia w bezpieczeństwie urządzeń mobilnych, odkąd urządzenia te zaczęły łączyć się z Internetem. Biorąc pod uwagę naszą nieustanną zależność od telefonów komórkowych oraz przekonanie, że niewielu cyberprzestępców dokonuje na nie ataków, istnieje duże prawdopodobieństwo zagrożeń w tym obszarze.

4. ATAK ZA POŚREDNICTWEM ZEWNĘTRZNEGO DOSTAWCY

Cyberprzestępcy preferują ścieżkę najmniejszego oporu. Serwer Microsoft Exchange padł ofiarą zmasowanego cyberataku w marcu 2021 roku. Zakłóciło to dziewięć agencji rządowych i 60 000 prywatnych firm.

5. ZANIEDBANIE PRAWIDŁOWEJ KONFIGURACJI

Narzędzia Big Data można dostosować do potrzeb organizacji. Firmy nadal zaniedbują znaczenie odpowiedniej konfiguracji ustawień bezpieczeństwa. Fifth Third Bank padł ofiarą jednego z największych naruszeń danych w 2020 r., z powodu zachowania dostępu dla byłego pracownika.

6. PRZESTARZAŁE OPROGRAMOWANIE ZABEZPIECZAJĄCE

Aktualizacja oprogramowania zabezpieczającego jest podstawową praktyką zarządzania technologią i jest obowiązkowa dla ochrony danych. Oprogramowanie zostało opracowane w celu ochrony przed znanymi zagrożeniami. Oznacza to, że każdy nowy złośliwy kod, który trafi do przestarzałego oprogramowania zabezpieczającego, pozostanie niewykryty.

7. INŻYNIERIA SPOŁECZNA

Cyberprzestępcy wiedzą, że techniki włamań szybko się przedawniają. Skupili się na niezawodnej, nietechnicznej socjotechnice, która opiera się na interakcjach społecznych i manipulacji psychologicznej, w celu uzyskania dostępu do poufnych danych. Ta forma włamania jest nieprzewidywalna i bardzo skuteczna.

8. BRAK SZYFROWANIA

Ochrona poufnych danych podczas przesyłania i przechowywania jest środkiem, który przyjęło niewiele branż, pomimo jej skuteczności. Branża opieki zdrowotnej obsługuje niezwykle wrażliwe dane i rozumie wagę ich utraty, dlatego wielu interesariuszy kładzie duży nacisk na szyfrowanie.

9. DANE FIRMOWE NA URZĄDZENIACH OSOBISTYCH

Niezależnie od tego, czy organizacja dystrybuuje telefony firmowe, czy nie, poufne dane są nadal dostępne na urządzeniach osobistych. Narzędzia do zarządzania urządzeniami mobilnymi ograniczają ich funkcjonalność, dlatego zabezpieczenie luk nie jest priorytetem dla wielu organizacji.

10. NIEODPOWIEDNIA TECHNOLOGIA BEZPIECZEŃSTWA

Inwestowanie w oprogramowanie do monitorowania bezpieczeństwa sieci stało się rosnącym trendem po bolesnych naruszeniach danych w 2014 r. Oprogramowanie zostało zaprojektowane aby ostrzegać o próbach włamania, ale te alerty są cenne tylko wtedy, gdy ktoś się do nich odniesie. Firmy zbyt mocno polegają na technologii, aby w pełni chronić się przed atakami.

Wyjątkowa norma bezpieczeństwa – ISO/IEC 27001

Legendarny rodowód

ISO/IEC 27001 wywodzi się z brytyjskiej normy BS 7799, napisanej przez brytyjski Departament Handlu i Przemysłu (DTI) i opublikowanej w 1995 roku.

CZĘŚĆ 1

Pierwsza część BS 7799, zawierająca najlepsze praktyki zarządzania bezpieczeństwem informacji, została zmieniona w 1998 roku.
Po wielu debatach między organami normalizacyjnymi na całym świecie, został przyjęty przez ISO i IEC i stał się ISO/IEC 17799 - Technologia informacyjna - Kodeks postępowania w zakresie zarządzania bezpieczeństwem informacji – w 2000 roku. Norma została zmieniona w 2005 r., razem z nieznaczną zmianą nazwy.
ISO i IEC ostatecznie włączyły tę część do rodziny ISO/IEC 27000 jako ISO/IEC 27002:2007.

CZĘŚĆ 2

Druga część, zatytułowana Systemy zarządzania bezpieczeństwem informacji – specyfikacja z wytycznymi dotyczącymi użytkowania – została po raz pierwszy opublikowana tuż przed 2000 r. Element ten koncentrował się na sposobie wdrożenia systemu zarządzania bezpieczeństwem informacji (SZBI), odnosząc się do potrzebnej struktury i zabezpieczeń. Następnie powstała z tego norma ISO/IEC 27001:2005.

CZĘŚĆ 3

Trzecia część została opublikowana w 2005 r. i obejmowała analizę ryzyka i zarządzanie nim. Jest zgodna z normą ISO/IEC 27001:2005.

ŁĄCZENIE CZĘŚCI 1–3

Po długim czasie, wprowadzeniu zmian i częściowej unifikacji, ISO i IEC stworzyły ISO/IEC 27001:2013 – uznany na całym świecie standard bezpieczeństwa informacji oparty na najlepszych praktykach, który pomaga organizacjom w utrzymaniu bezpieczeństwa własności intelektualnej i zasobów informacyjnych.

Znaczenie certyfikacji ISO/IEC 27001

Używana przez dziesiątki tysięcy organizacji, certyfikacja ISO/IEC 27001 pokazuje zaangażowanie organizacji w bezpieczeństwo informacji i daje pewność klientom i innym partnerom, że poważnie traktuje ochronę informacji znajdujących się pod jej kontrolą.

Standard jest niezależny od technologii, więc nie ma znaczenia, jakie środowisko technologiczne posiadasz. Jest napisany w taki sposób, że każda organizacja, od małych firm po duże wielomiliardowe przedsiębiorstwa, może z niego korzystać.

ISO/IEC 27001 określa wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia SZBI w zakresie bezpieczeństwa i ochrony. Obejmuje również wymagania dotyczące oceny i postępowania z zagrożeniami bezpieczeństwa informacji, dostosowane do Twoich potrzeb.

Ponieważ jest to standard systemu zarządzania, jest zgodny z innymi uznanymi na całym świecie standardami, takimi jak:

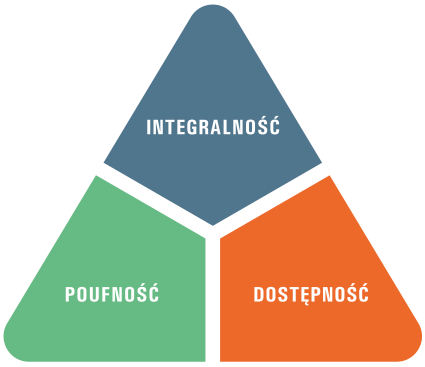
- ISO/IEC 27701 (zarządzanie informacjami o prywatności)
- ISO/IEC 20000-1 (zarządzanie usługami IT)
- ISO 22301 (ciągłość działania)
- ISO 9001 (jakość)
- ISO 14001 (środowiskowy)
- ISO 45001 (BHP)

Ta zgodność pozwala wdrożyć wymagania kilku z tych standardów w organizacji przy minimalnym wysiłku, jednocześnie korzystając z efektów synergii.

Na podstawie triady CIA

Wdrożenie SZBI pokazuje twoje zaangażowanie w ochronę poufności, integralności i dostępności (CIA) informacji znajdujących się pod twoją kontrolą.

Standard jest zgodny z Triadą CIA, która zapewnia istotne funkcje bezpieczeństwa. Pomaga uniknąć problemów ze zgodnością, wspiera ciągłość biznesową i zapobiega utracie reputacji.



Oznacza to, że ISO/IEC 27001 obejmuje:

- Polityki bezpieczeństwa informacji
- Bezpieczeństwo komunikacji
- Organizacja bezpieczeństwa informacji
- Relacje z dostawcami
- Pozyskiwanie, rozwój i utrzymanie systemu
- Zarządzanie aktywami
- Bezpieczeństwo zasobów ludzkich
- Kontrolę dostępu
- Zarządzanie incydentami bezpieczeństwa informacji
- Kryptografię
- Zgodność (Compliance)
- Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania
- Bezpieczeństwo fizyczne i środowiskowe
- Bezpieczeństwo operacji

Jakie są najważniejsze korzyści?

ISO/IEC 27001 może prowadzić do:

- Zwiększonej wiarygodności
- Zmniejszonego ryzyka oszustw, utraty informacji i ujawnienia
- Demonstracji integralności systemu
- Transformacji kultury biznesowej i większej świadomość znaczenia bezpieczeństwa informacji
- Nowych możliwości biznesowych dzięki klientom dbającym o bezpieczeństwo
- Silniejszego pojęcia poufności w całej organizacji
- Lepszego przygotowania na nieuniknione – kolejne zdarzenie lub incydent związany z bezpieczeństwem

Ewolucja w celu sprostania zagrożeniom

Czas na aktualizację

ISO/IEC 27001 została ostatnio zaktualizowana w 2013 r., a cyberświat i jego zagrożenia dramatycznie ewoluowały, stając się coraz bardziej złożone dzięki bardziej innowacyjnej technologii, operacjom w chmurze i biznesowi online. Standard musi podążać za nim i być plastycznym, aby pomieścić aktualizacje.

15 lutego 2022 roku był dniem przełomowym. Opublikowano normę ISO/IEC 27002:2022 – Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Kontrola bezpieczeństwa informacji. Z tego powodu załącznik A do normy ISO/IEC 27001 wymagał aktualizacji w celu dostosowania do zabezpieczeń ISO/IEC 27002:2022.

Główne zmiany w ISO/IEC 27001:2022

TYTUŁ

Nazwa została zmieniona, aby odzwierciedlić prawdziwy zakres normy ISO/IEC 27001:2022 – Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Systemy zarządzania bezpieczeństwem informacji – Wymagania.
Jest to również zgodne z nowym tytułem ISO/IEC 27002:2022.

NUMERACJA KLAUZUL

Wprowadzono nowe podrozdziały w celu dalszej harmonizacji struktury dokumentu z innymi standardami systemów zarządzania, takimi jak ISO 9001 i ISO 22301.
Dwa podrozdziały – 10.1 i 10.2 – również zostały zamienione.
10.1 to ciągłe doskonalenie, a 10.2 to niezgodność i działania korygujące.
Nie ma żadnych zmian w ich wymaganiach.

NOWY TEKST

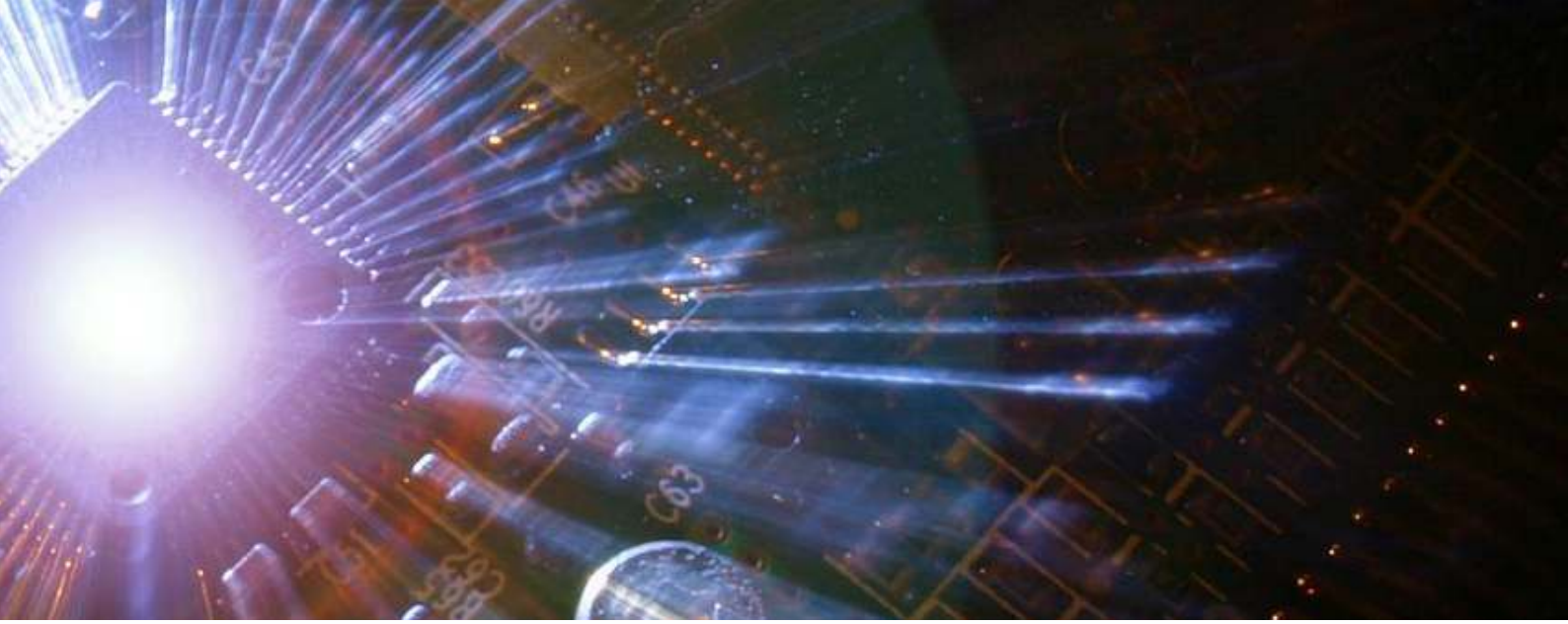
Chociaż dodano nowy tekst i wprowadzono parę zmian, zmiany te tylko wyjaśniają wymagania i nie dodają nowych do standardu.

ZAŁĄCZNIK A

Załącznik A nosi teraz tytuł Odniesienie do zabezpieczeń bezpieczeństwa informacji, a zabezpieczenia zostały zmienione w celu dostosowania do ISO/IEC 27002:2022. W wydaniu 2013 tylko opisy zabezpieczeń pochodzą z ISO/IEC 27002.

INNE ZMIANY

Wprowadzono też aktualizacje kilku klauzul.



Silne więzi rodzinne

Główne zmiany w ISO/IEC 27002:2022

Jak wspomniano, wiele aktualizacji ISO/IEC 27001 wynika z ewolucji ISO/IEC 27002. Poniżej znajduje się podsumowanie zmian tego ostatniego.

LICZBA ZABEZPIECZEŃ

ISO/IEC 27002:2022 ma 93 elementy w porównaniu ze 114 w wersji z 2013 roku.

KATEGORIE ZABEZPIECZEŃ

Zabezpieczenia są pogrupowane w cztery kategorie – organizacyjną, ludzką, fizyczną i technologiczną – zamiast 14 tematów i 36 kategorii w edycji 2013.

Układ czterech kategorii podkreśla, że ochrona informacji i danych to coś więcej niż tylko środki technologiczne. Aby osiągnąć wyniki w zakresie bezpieczeństwa informacji, zabezpieczenia technologiczne są tylko środkami zaradczymi zapobiegającymi lub łagodzącymi zagrożenia bezpieczeństwa informacji.

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

Poza tym, ten nowy układ kontroli może ułatwić kierownictwu przypisanie obowiązków w organizacji, aby poprawić bezpieczeństwo informacji.

NOWE ZABEZPIECZENIA

Istnieje 11 nowych zabezpieczeń w odpowiedzi na ewolucję technologii i praktyk branżowych:

1. Analiza zagrożeń
2. Bezpieczeństwo informacji podczas korzystania z usług w chmurze
3. Gotowość ICT do ciągłości działania
4. Monitorowanie bezpieczeństwa fizycznego
5. Zarządzanie konfiguracją
6. Usuwanie informacji
7. Maskowanie danych
8. Zapobieganie wyciekom danych
9. Działania monitorujące
10. Filtrowanie stron internetowych
11. Bezpieczne kodowanie

SCALONE ZABEZPIECZENIA

Dwadzieścia cztery zabezpieczenia w edycji 2022 są wynikiem połączenia niektórych z wersji 2013. Scalanie oznacza mniejszą liczbę zabezpieczeń, a tym samym szczuplejszy standard.

Konkluzja

ISO/IEC 27001 jest standardem potwierdzającym swoja skuteczność w miarę ewolucji zagrożeń cybernetycznych. Wiele powodów, w tym nasilające się zagrożenia, postęp technologiczny i doskonała łączność, taka jak 5G, może sprawić, że Twoja firma stanie się celem cyberprzestępców.

Zmiany te rzeczywiście rodzą zmiany. Kluczową zaletą ISO/IEC 27001 jest jej zdolność do dotrzymywania kroku w ciągle zmieniającym się cyberświecie.

Chociaż aktualizacje w wersji z 2022 r. sprawiają, że dokumentacja i wytyczne są cięższe i dodają więcej obowiązków, istnieją jasne i szczegółowe wyjaśnienia każdego zabezpieczenia.

Zgodnie z oczekiwaniami najbardziej znaczącą zmianą są zmiany załącznika A w celu dostosowania ich do zabezpieczeń bezpieczeństwa ISO/IEC 27002:2022.

Zmiany w klauzulach 4–10 są drobnymi zmianami redakcyjnymi mającymi na celu dalszą harmonizację struktury z innymi standardami systemu zarządzania.

Jeśli Twoja organizacja jest już zgodna z ISO/IEC 27001, nie są potrzebne żadne zmiany technologiczne, a jedynie aktualizacje w dokumentacji. Może być konieczne poprawienie zasad wewnętrznych zgodnie z nowymi klauzulami podrzędnymi i zmodyfikowanymi wymaganiami. Należy również dokonać przeglądu wyników oceny ryzyka i planów postępowania z ryzykiem oraz aktualizacja deklaracji stosowania (SoA).

Jak możemy pomóc

Możemy Ci pomóc, niezależnie od tego, czy chcesz płynnego przejścia, czy pierwszej certyfikacji zgodnie z normą ISO/IEC 27001:2022. Stworzyliśmy pakiet usług i materiałów, w tym szkolenia przejściowe i wytyczne dotyczące aktualizacji ISO/IEC 27001 i ISO/IEC 27002.

Możemy zapewnić, że dostosowałeś dokumentację w okresie przejściowym. W związku z tym nie trzeba planować nowych audytów, ponieważ będą one miały miejsce podczas regularnych audytów nadzoru. Ponadto wymagany będzie dodatkowy czas na ocenę pomyślnego przejścia zgodnie z Międzynarodowym Forum Akredytacyjnym (IAF) dokument MD 26:2022

Jednak po odnowieniu certyfikatu w okresie przejściowym możesz pracować nad nowymi zabezpieczeniami, aby uniknąć pozostawienia ich na ostatnią chwilę.

Niezależnie od tego, czy jesteś obecnym klientem, czy nowym użytkownikiem ISO/IEC 27001, możemy wesprzeć Cię w procesie zmian i certyfikacji.

www.sgs.pl

pl.certyfikacja@sgs.com

ATRYBUTY

ISO/IEC 27002:2022 wprowadza atrybuty dla każdego zabezpieczenia. Każda zabezpieczenie jest skojarzone z pięcioma atrybutami o odpowiadających im wartościach.

1. Rodzaje zabezpieczeń – prewencyjne, wykrywcze, korekcyjne.
2. Właściwości bezpieczeństwa informacji – poufność, integralność, dostępność.
3. Koncepcje cyberbezpieczeństwa – identyfikacja, ochrona, wykrywanie, reagowanie, odzyskiwanie.
4. Możliwości operacyjne – zarządzanie, zarządzanie zasobami, ochrona informacji, bezpieczeństwo zasobów ludzkich, bezpieczeństwo fizyczne, bezpieczeństwo systemu i sieci, bezpieczeństwo aplikacji, bezpieczna konfiguracja, zarządzanie tożsamością i dostępem, zarządzanie zagrożeniami i lukami w zabezpieczeniach, ciągłość, bezpieczeństwo relacji z dostawcami, prawo i zgodność, zarządzanie zdarzeniami bezpieczeństwa informacji, zapewnienie bezpieczeństwa informacji.
5. Dziedziny bezpieczeństwa – zarządzanie i ekosystem, ochrona, obrona, odporność.

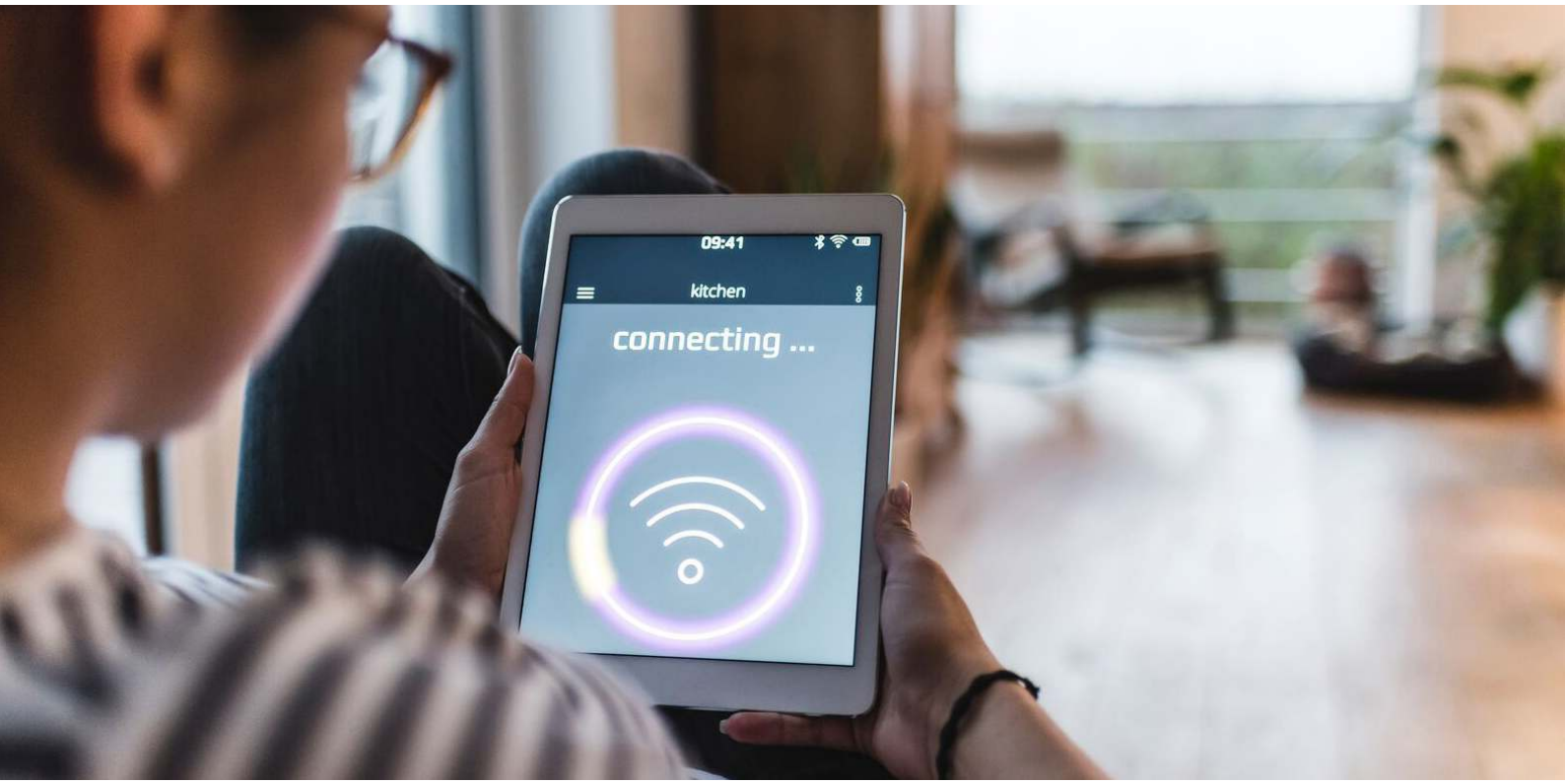
POWÓD ZASTĘPUJE CEL

Wersja 2022 używa powodu, a nie celu. Każde zabezpieczenie ma zdefiniowany powód, aby zilustrować, dlaczego zabezpieczenie powinno zostać zaimplementowane.

INNE ZMIANY

Tytuł obejmuje teraz bezpieczeństwo informacji, cyberbezpieczeństwo i ochronę prywatności - zabezpieczenia bezpieczeństwa informacji, aby odzwierciedlić zakres standardu. Kodeks postępowania został usunięty, aby wskazać, że dokument jest odniesieniem do ogólnych zabezpieczeń bezpieczeństwa informacji.

ISO/IEC 27000 nie jest już normatywnym odniesieniem do ISO/IEC 27002:2022. Zamiast tego zastosowanie mają terminy i definicje zawarte w klauzuli 3 z 2022 r. Użytkownikom wydania z 2022 r. zaleca się zapoznanie się z jej terminami i definicjami, aby ułatwić im zrozumienie mechanizmów zabezpieczeń i wskazówek zawartych w dokumencie.



Pionier ochrony od dziesięcioleci

Dzięki doświadczeniu we wszystkich branżach wiemy, co bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności, a także inne kwestie cyfrowe, oznaczają dla organizacji, niezależnie od ich wielkości, zakresu działalności i złożoności.

Nasze stale ewoluujące portfolio może poprawić Twoją wydajność, jednocześnie prowadząc Cię do zgodności z przepisami uznawanymi na całym świecie. Nasze systemy certyfikacji obejmują wiele obszarów, w tym przetwarzanie i ochronę danych, przechowywanie w chmurze, bezpieczeństwo obiektów i loterii oraz reagowanie na zdarzenia o znaczeniu krytycznym dla biznesu.

Niektóre kluczowe usługi

CERTYFIKACJA ISO/IEC 27001

Certyfikacja jest dowodem niezależnego przeglądu skutecznego wdrożenia solidnego SZBI opartego na najlepszych praktykach. Dostarcza ona pewność wewnątrz organizacji i, co ważniejsze, partnerom biznesowym, że Twoja firma poważnie traktuje bezpieczeństwo informacji, cyberbezpieczeństwo i prywatność, a także wykazuje zaangażowanie na poziomie najwyższego kierownictwa.

CERTYFIKACJA ISO/IEC 27701

ISO/IEC 27701, rozszerzenie ISO/IEC 27001, dotyczy ochrony informacji o prywatności, takich jak data urodzenia i krajowe numery identyfikacyjne. System zarządzania informacjami o prywatności (PIMS) zapewnia administratorom oraz podmiotom przetwarzającym ramy do zarządzania danymi osobowymi (PII).

Certyfikacja umożliwia organizacji skuteczne wdrażanie zgodności z nowymi wymogami regulacyjnymi i przepisami dotyczącymi prywatności danych osobowych na całym świecie.

SZKOLENIE

Nasi doświadczeni instruktorzy zapewniają spójne, skuteczne i wysokiej jakości szkolenia, aby zapewnić, że Twoi pracownicy mają najlepsze kwalifikacje do doskonalenia Twojej organizacji. Nasze metody szkoleniowe obejmują szkolenia otwarte, wewnętrzne, e-learning, wirtualne i hybrydowe.

Zrozumienie ISO/IEC 27001:2022, jej aktualizacji i okresu przejściowego może być dezorientujące. Stworzyliśmy Transition Training Course, który zawiera szczegółowe porównania i opisy zmian. Jest to część kompleksowego portfolio szkoleń cyfrowych.

INNE ROZWIĄZANIA CERTYFIKACYJNE I SZKOLENIOWE

Należą do nich:

- ISO/IEC 20000 – Zarządzanie usługami IT (ISMS)
- ISO 22301 – Systemy zarządzania ciągłością działania (BCMS)
- ISO/IEC 27017– Kodeks postępowania w zakresie kontroli bezpieczeństwa informacji oparty na normie ISO/IEC 27002 dla usług w chmurze
- ISO/IEC 27018 – Kodeks postępowania w zakresie ochrony PII w chmurach publicznych działających jako procesory PII
- ISO/IEC 27701 – Kodeks postępowania w zakresie zarządzania informacją o prywatności (PIMS)
- KSC (Krajowy System Cyberbezpieczeństwa)
- ISO/IEC 19770 – Systemy zarządzania zasobami IT (ITAM)
- EN 50600 / ISO/IEC 22237 – Wyposażenie i infrastruktura Data Center
- Cloud Security Alliance (CSA) Security, Trust, Assurance and Risk (STAR)

Odwołania

Forbes – https://www.forbes.com/sites/bernardmarr/2022/03/18/the-biggest-cyber-security-risks-in-2022/?sh=7994336c7d7b

Uniwersytet Georgetown (USA) – https://scsonline.georgetown.edu/programs/masters-technology-management/resources/top-threats-to-information-technology

Sprawy prywatności – https://www.privacyaffairs.com/cybersecurity-attacks-in-2021/

Siła tożsamości – https://www.identityforce.com/blog/2020-data-breaches

ISMS.online – https://www.isms.online/iso-27001/

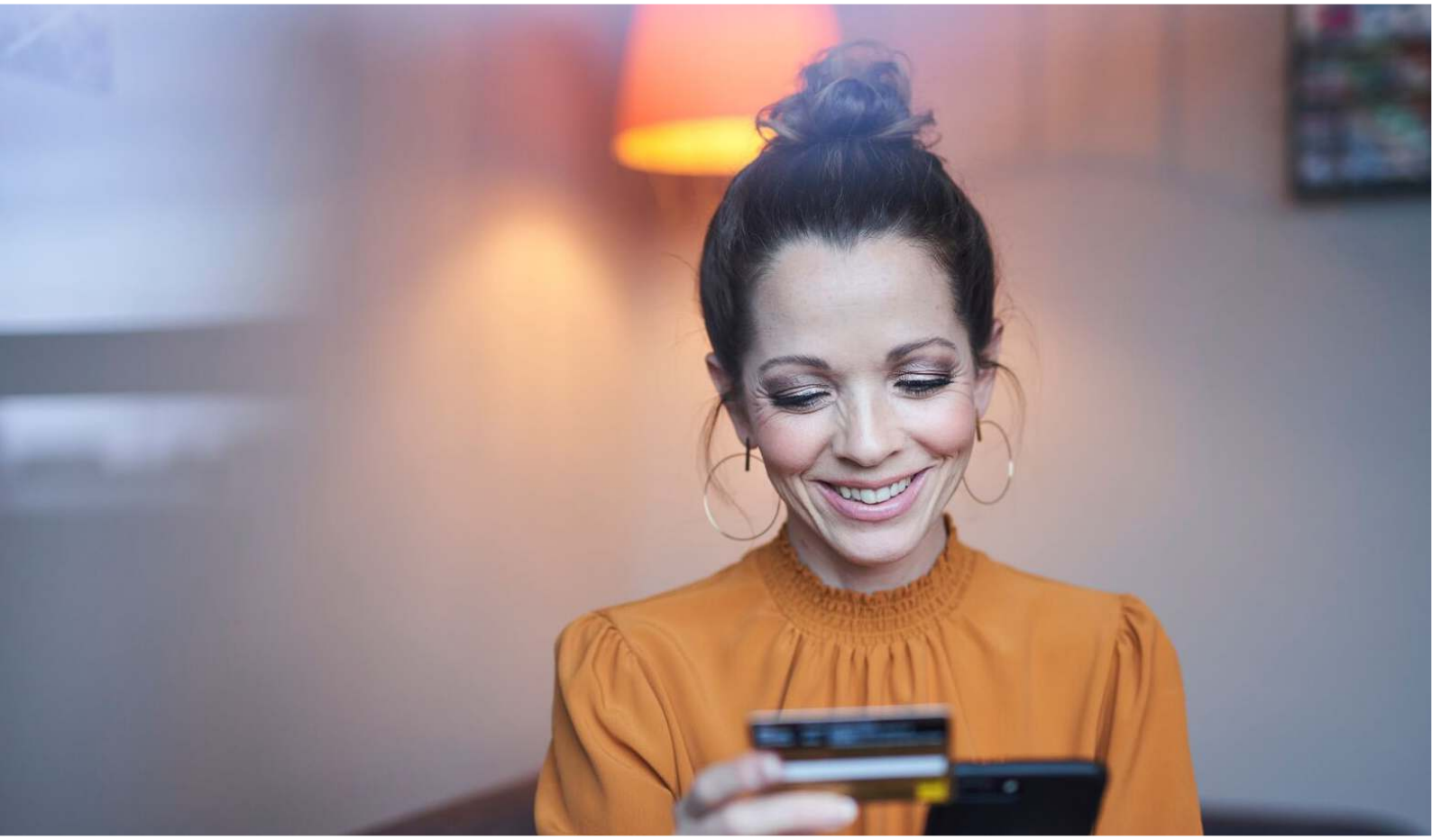
CISCO – https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html

https://www.cisco.com/c/en_uk/products/security/what-is-cybersecurity.html

SGS – www.sgs.pl

ISO – https://www.iso.org

IAF – https://iaf.nu/iaf_system/uploads/documents/IAF_MD_26_Transition_requirements_for_ISOIEC_27001-2022_09082022.pdf



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