

EN ISO/IEC 27006:2020

Spis treści

Przedmowa do Normy Europejskiej	4
Wprowadzenie	5
1 Zakres normy	6
2 Powołania normatywne	6
3 Terminy i definicje	6
4 Zasada Metody	6
5 Wymagania ogólne	7
5.1 Zagadnienia prawne i związane z umową	7
5.2 Zarządzanie bezstronnością	7
5.2.1 IS 5.2 Konflikt interesów	7
5.3 Zobowiązania i finansowanie	7
6 Wymagania dotyczące struktury	7
7 Wymagania dotyczące zasobów	8
7.1 Kompetencje personelu	8
7.1.1 IS 7.1.1 Postanowienia ogólne	8
7.1.2 IS 7.1.2 Określenie kryteriów kompetencyjnych	8
7.2 Personel zaangażowany w działalność certyfikacyjną	12
7.2.1 IS 7.2 Wykazywanie wiedzy i doświadczenia audytorów	12
7.3 Korzystanie z indywidualnych audytorów zewnętrznych i zewnętrznych ekspertów technicznych	13
7.3.1 IS 7.3 Wykorzystanie zewnętrznych audytorów lub zewnętrznych ekspertów technicznych jako części zespołu audytującego	13
7.4 Zapisy dotyczące personelu	13
7.5 Zlecanie na zewnątrz	13
8 Wymagania dotyczące informacji	13
8.1 Informacje publiczne	13
8.2 Dokumenty certyfikacji	14
8.2.1 IS 8.2 Dokumenty certyfikacji SZBI	14
8.3 Powoływanie się na certyfikację i stosowanie znaków	14
8.4 Poufność	14
8.4.1 IS 8.4 Dostęp do zapisów organizacji	14
8.5 Wymiana informacji pomiędzy jednostką certyfikującą a jej klientami	14
9 Wymagania dotyczące procesu	14
9.1 Działania przed certyfikacją	14
9.1.1 Wniosek	14
9.1.2 Przegląd wniosku	15
9.1.3 Program audytu	15
9.1.4 Określenie czasu audytu	16
9.1.5 Próbkowanie z wielu lokalizacji	16
9.1.6 Systemy zarządzania według wielu norm	17
9.2 Planowanie audytów	18
9.2.1 Określanie celów, zakresu i kryteriów audytu	18
9.2.2 Wybór i powołanie zespołu audytującego	18
9.2.3 Plan audytu	18

9.3	Certyfikacja początkowa	19
9.3.1	IS 9.3.1 Audyt certyfikacji początkowej	19
9.4	Przeprowadzanie audytów	20
9.4.1	IS 9.4 Postanowienia ogólne	20
9.4.2	IS 9.4 Specyficzne elementy audytu SZBI	20
9.4.3	IS 9.4 Raport z audytu	21
9.5	Decyzja o certyfikacji	21
9.5.1	IS 9.5 Decyzja o certyfikacji	21
9.6	Utrzymywanie certyfikacji	22
9.6.1	Postanowienia ogólne	22
9.6.2	Działania w nadzorze	22
9.6.3	Ponowna certyfikacja	23
9.6.4	Audyty specjalne	23
9.6.5	Zawieszanie, cofanie lub ograniczanie zakresu certyfikacji	23
9.7	Odwołania	23
9.8	Skargi	23
9.8.1	IS 9.8 Skargi	23
9.9	Zapisy dotyczące klientów	24
10	Wymagania dotyczące systemu zarządzania jednostek certyfikujących	24
10.1	Opcje	24
10.1.1	IS 10.1 Wdrożenie SZBI	24
10.2	Opcja A: Ogólne wymagania dotyczące systemu zarządzania	24
10.3	Opcja B: Wymagania dotyczące systemu zarządzania wg ISO 9001	24
	Załącznik A (informacyjny) Wiedza i umiejętności wymagane do audytowania i certyfikacji SZBI	25
	Załącznik B (normatywny) Czas audytu	27
	Załącznik C (informacyjny) Metody obliczania czasu audytu	32
	Załącznik D (informacyjny) Wytyczne dotyczące przeglądu wdrożonych zabezpieczeń wg ISO/IEC 27001:2013, Załącznik A	37
	Bibliografia	51