Certyfikacja NASK

Program certyfikacji Firma Bezpieczna Cyfrowo (PC-FBC)

(Egzemplarz dla Klienta)

Wersja **1.2** (data wydania 10.10.2023)

NASK-PIB
ul. Kolska 12
01–045 Warszawa

NIP: 521 04 17 157
Regon: 010464542
KRS: 0000012938

nask@nask.pl
+48 22 380 82 00
www.nask.pl

Certyfikacja NASK

Spis treści

Certyfikacja NASK

Informacje o programie certyfikacji

Właściciel programu	NASK-PIB NASK Państwowy Instytut Badawczy
Patronat	Ministerstwo Cyfryzacji Ministerstwo Rozwoju i Technologii

Opis programu

Program certyfikacji cyberbezpieczeństwa dla biznesu Firma Bezpieczna Cyfrowo jest elementem systemu oceny zgodności i certyfikacji cyberbezpieczeństwa, w szczególności dotyczy:

- małych i średnich przedsiębiorstw (MŚP),
- certyfikacji procesu[1].

Informacja i zastrzeżenie: Program certyfikacji jest inspirowany przez program certyfikacji CyberEssentials, opracowany, wdrożony i stosowany w Wielkiej Brytanii. Nie należy utożsamiać obu programów pomimo istniejących podobieństw. Program w obecnej wersji nie jest akredytowany.

[1] W rozumieniu normy PN-EN ISO/IEC 17065:2013 – Wymagania dla jednostek certyfikujących wyroby, procesy lub usługi.

Certyfikacja NASK

1. Cel i zakres stosowania

Niniejszy program certyfikacji stosuje się do prowadzenia oceny i certyfikacji oraz nadzoru nad certyfikatem w Jednostce Certyfikującej Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytucie Badawczym (NASK – PIB).

Celem programu jest określenie zasad realizacji procesu certyfikacji cyberbezpieczeństwa małych i średnich przedsiębiorstw (MŚP) poprzez niezależną ocenę zgodności z wymaganiami określonymi przez jednostkę certyfikującą i zgodnie z przyjętą w programie metodyką oceny.

Proces certyfikacji ma zapewnić, że proces zarządzania cyberbezpieczeństwem w firmach przystępujących do programu jest atestowany na zgodność z wyspecyfikowanymi wymaganiami przez niezależną stronę trzecią.

Certyfikacja procesu jest dobrowolna. Usługi te są otwarte dla wszystkich podmiotów w sposób niedyskryminujący kogokolwiek.

NASK – PIB gwarantuje, że działania dotyczące certyfikacji realizowane są w sposób bezstronny i posiada zasoby adekwatne do przeprowadzenia procesu certyfikacji.

Niniejszy program certyfikacji Firma Bezpieczna Cyfrowo jest udostępniany poprzez stronę internetową firmabezpiecznacyfrowo.pl.

MŚP będą zaakceptowane do procesu certyfikacji, jeśli zakres wnioskowanej certyfikacji jest zgodny z możliwościami programu oraz kryteriami oceny.

Certyfikat wydany dla MŚP jest poświadczeniem przez jednostkę certyfikującą, że procesy zarządzania cyberbezpieczeństwem w danym podmiocie spełniają wymagania określone w programie certyfikacji.

Odpowiedzialność za realizowany proces zawsze ponosi jego właściciel (jeżeli jest na terenie UE), a jeżeli siedziba przedsiębiorstwa mieści się poza UE – odpowiedzialność ponosi upoważniony przedstawiciel na terenie UE[2].

Wydany certyfikat w żaden sposób nie przenosi odpowiedzialności lub jej części na jednostkę certyfikującą.

2. Dokumenty powiązane

PN-EN ISO/IEC 17065 Ocena zgodności. Wymagania dla jednostek certyfikujących wyroby, procesy i usługi.

PN-EN ISO/IEC17067 Ocena zgodności. Podstawy certyfikacji wyrobów oraz wytyczne dotyczące programów certyfikacji wyrobów.

PN-EN ISO/IEC 17000 Ocena zgodności - Terminologia i ogólne zasady.

PN-ISO/IEC 17007:2012 - Ocena zgodności - Wytyczne dotyczące redagowania dokumentów normatywnych właściwych do stosowania w ocenie zgodności.

[2] Do udziału w pilotażu programu (wrzesień - grudzień 2023 r.) kwalifikowane są wyłącznie MŚP mające siedzibę w Polsce (osoba prawna) lub miejsce zamieszkania w Polsce (osoba fizyczna).

PN-EN ISO/IEC 17020:2012 - Ocena zgodności - Wymagania dotyczące działania różnych rodzajów jednostek przeprowadzających inspekcje.

PN-EN ISO 9001 Systemy zarządzania jakością. Wymagania.

ISO/IEC 27001 Technika Informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji – Wymagania.

ISO/IEC 27002 Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady zabezpieczania informacji.

ISO/IEC 27005 Technika informatyczna - Techniki bezpieczeństwa - Zarządzanie ryzykiem w bezpieczeństwie informacji.

ISO 31000 Zarządzanie ryzykiem – Wytyczne.

PN-ISO/IEC 17030:2009 Ocena zgodności – Wymagania ogólne dotyczące znaków zgodności strony trzeciej.

Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku.

Cyber Essentials: Requirements for IT infrastructure, v3.1, April 2023.

Cyber Essentials Readiness Tool https://getreadyforcyberessentials.iasme.co.uk/.

Poradnik Firma Bezpieczna Cyfrowo: https://firmabezpiecznacyfrowo.pl/poradnik/

3. Definicje

Dla potrzeb niniejszego dokumentu, dokumentów powiązanych i wniosku o certyfikację stosuje się następujące definicje:

atestacja – wystawienie oświadczenia opartego na decyzji poprzedzonej przeglądem, że spełnienie wyspecyfikowanych wymagań zostało wykazane,

bezstronność – zachowanie obiektywności,

certyfikacja – atestacja przez stronę trzecią w odniesieniu do wyrobów, procesów lub usług,

certyfikat – wydany przez NASK-PIB dokument poświadczający, że przeprowadzony przez NASK-PIB proces certyfikacji został zakończony z wynikiem pozytywnym,

cyberbezpieczeństwo – działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami,

cofnięcie – unieważnienie oświadczenia o zgodności,

jednostka certyfikująca – jednostka oceniająca zgodność jako strona trzecia, działająca w programach certyfikacji; w przypadku niniejszego programu oznacza NASK – PIB,

kierownik jednostki certyfikującej – Dyrektor ds. Certyfikacji NASK-PIB,

klient – organizacja lub osoba odpowiedzialna wobec jednostki certyfikującej za zapewnienie, że wymagania certyfikacyjne są spełnione,

nadzór – systematyczne powtarzanie działań związanych z oceną zgodności jako podstawa do utrzymania ważności oświadczenia o zgodności,

niezgodność – niespełnienie wymagania,

ocena – niezależny, udokumentowany proces uzyskiwania dowodów, w celu określenia stopnia spełnienia wymagań, stanowiących kryteria certyfikacji,

odwołanie – wystąpienie przez klienta do jednostki certyfikującej o ponowne rozpatrzenie przez tę jednostkę decyzji przez nią podjętej,

organizacja (firma) – oznacza małego lub średniego przedsiębiorcę (MŚP) w rozumieniu Ustawy z dnia 4 lipca 2004 r. o swobodzie działalności gospodarczej,

proces – zbiór działań wzajemnie powiązanych lub wzajemnie oddziałujących, które przekształcają wejścia w wyjścia,

proces do oceny – realizowany w MŚP proces wdrażania odpowiednich środków technicznych i organizacyjnych składających się na cyberbezpieczeństwo w MŚP, o którego certyfikację klient wnioskuje,

program certyfikacji – system certyfikacji odnoszący się do określonych wyrobów, procesów i usług, do których mają zastosowanie te same wyspecyfikowane wymagania,

skarga – wyrażenie niezadowolenia innego niż zastrzeżenie, przez jakąkolwiek osobę lub organizację, w stosunku do jednostki certyfikującej dotyczące działań tej jednostki, wymagające odpowiedzi,

system informatyczny – zestaw elementów sprzętu (hardware), programów (software), danych i użytkowników, które w połączeniu zapewniają możliwość przechowywania, transmisji, przetwarzania i odtwarzania informacji,

umowa – umowa o świadczenie usług certyfikacyjnych zawarta między NASK-PIB a klientem, która obejmuje wykonanie przez NASK-PIB na zlecenie klienta usług certyfikacyjnych,

wniosek o certyfikację – standardowy formularz wypełniany przez klienta, określający zakres usług certyfikacyjnych, jakie ma wykonać jednostka certyfikująca, wraz ze wszelkimi innymi informacjami dotyczącymi wykonania usług certyfikacyjnych na warunkach wskazanych w umowie,

zakres certyfikacji – zidentyfikowanie: wyrobu, procesu lub usługi w odniesieniu do których certyfikacja jest udzielona; programu certyfikacji i dokumentów normatywnych, z którymi ocenia się zgodność.

3. Wymagania certyfikacyjne i metodyka oceny

3.1 Wymagania certyfikacyjne

Wymagania certyfikacyjne w niniejszym programie określają:

1) Program certyfikacji Firma Bezpieczna Cyfrowo (PC-FBC),
2) Specyfikacja techniczna - Wymagania dla Programu certyfikacji Firma Bezpieczna Cyfrowo.

3.2 Metodyka oceny

Metodykę oceny stanowi dokument Metodyka oceny dla Programu certyfikacji Firma Bezpieczna Cyfrowo.

4. Przebieg procesu certyfikacji

4.1 Etapy procesu certyfikacji Firma Bezpieczna Cyfrowo

4.1.1 Wniosek o certyfikację

Klient (przedsiębiorca z grupy MŚP) zainteresowany uzyskaniem certyfikatu przesyła wniosek o certyfikację wraz z dokumentami wymaganymi do przeprowadzenia procesu certyfikacji do jednostki certyfikującej poprzez system ePUAP.

Formularz wniosku wraz ze wszystkimi wymaganymi wzorami oświadczeń dostępny jest na stronie internetowej programu Firma Bezpieczna Cyfrowo oraz w jednostce certyfikującej.

Klient może otrzymać na życzenie informacje o szczegółach procedury certyfikacji w ramach programu Firma Bezpieczna Cyfrowo, normach lub innych dokumentach kryterialnych dotyczących certyfikacji oraz informacje odnoszące się do dokumentacji wymaganej w procesie certyfikacji.

We wniosku wymagane jest w szczególności podanie następujących informacji o kliencie tj.:

- dane identyfikacyjne podmiotu, wraz z numerem identyfikacji podatkowej lub innym numerem właściwym dla wnioskującego,
- imię i nazwisko osoby lub grupy osób umocowanych do złożenia wniosku o certyfikację,
- oświadczenia o zapoznaniu się z i akceptacja mających zastosowanie warunków i wymagań wnioskowanej certyfikacji,
- listę siedzib, oddziałów i obiektów, wraz z ich lokalizacjami, gdzie prowadzony jest proces będący przedmiotem oceny,
- potwierdzenie wykonania opłaty za rozpatrzenie wniosku.

4.1.2. Przegląd dokumentów i umowa

Jednostka certyfikująca dokonuje przeglądu wniosku (weryfikacja dokumentacji, określenie ewentualnych braków). W przypadku kompletności złożonych dokumentów następuje podpisanie umowy o certyfikację. Wzór umowy jest dostępny na stronie internetowej programu Firma Bezpieczna Cyfrowo.

Niniejszy program jest integralną częścią tej umowy, która szczegółowo reguluje prawa i obowiązki jednostki certyfikującej i klienta.

W przypadku braku kompletności dokumentacji klient zostaje wezwany do ich uzupełnienia w czasie nie dłuższym niż 14 dni. Niepoprawione wnioski pozostawia się bez dalszego rozpatrzenia.

Warunkiem rozpoczęcia procesu jest zapoznanie się z Poradnikiem Firma Bezpieczna Cyfrowo, wypełnienie przez klienta ankiety samooceny oraz wniesienie opłaty za

rozpatrzenie wniosku. Ankieta samooceny oraz ww. poradnik dostępne są na stronie internetowej programu Firma Bezpieczna Cyfrowo a szczegółowe dane dotyczące opłat podano w pkt. 7 programu.

Klient jest zobowiązany do aktualizacji dokumentacji i materiału zawartego we wniosku o certyfikację przekazanych jednostce certyfikującej, jeśli wystąpią w nich zmiany podczas rozpatrywania wniosku.

4.1.3 Ocena

Przedmiotem oceny jest *proces wdrożenia odpowiednich środków technicznych i organizacyjnych składających się na cyberbezpieczeństwo w MŚP*: tj. od wypełnienia ankiety diagnostycznej, zapoznania się z materiałami edukacyjnymi dostępnymi na stronie internetowej programu Firma Bezpieczna Cyfrowo poprzez zapoznanie się ze specyfikacją wymagań dla programu Firma Bezpieczna Cyfrowo, implementację odpowiednich środków technicznych i organizacyjnych zapewniających cyberbezpieczeństwa, złożenie wniosku certyfikacyjnego, wypełnienie kwestionariusza oceny zgodnie z wymaganiami jednostki certyfikującej do uzyskania certyfikatu (patrz Diagram 1).

W zakresie pozyskiwania dowodów na spełnienie wymagań jednostka certyfikująca prowadzi weryfikację kwestionariusza i oświadczeń złożonych przez klienta. Może w tym celu (jeśli dotyczy) wykonywać przewidziane w procedurze certyfikacji działania związane z oceną (np. testy lub inspekcje) wykonywane za pomocą środków komunikacji na odległość. Procedura oceny jest dostępna w jednostce certyfikującej na życzenie klienta.

Jednostka certyfikująca weryfikuje wdrożenie następujących środków organizacyjnych i technicznych służących zapewnieniu cyberbezpieczeństwa:

1) **Zakres oceny**
   W celu określenia obszaru podlegającego ocenie organizacja powinna zidentyfikować swoją działalność w zakresie eksploatowanych technologii ICT, zidentyfikować aktywa oraz usługi stron trzecich,

2) **Zabezpieczenie brzegowe (Firewall)**
   W celu zapewnienia bezpieczeństwa usług dostępnych z Internetu organizacja powinna zapewnić zabezpieczenie każdego urządzenia w sieci firmy za pomocą prawidłowo skonfigurowanego firewall,

3) **Bezpieczna konfiguracja**
   W celu zapewnienia odpowiedniej konfiguracji sprzętu biurowego oraz urządzeń sieciowych organizacja powinna proaktywnie zarządzać bezpieczeństwem ICT w zakresie komputerów firmowych i urządzeń sieciowych,

4) **Zarządzanie aktualizacjami**
   W celu zapewnienia bezpiecznego korzystania z urządzeń i instalowanego na nich oprogramowania, organizacja powinna zapewnić, że całe wykorzystywane oprogramowanie jest aktualizowane,

5) **Kontrola dostępu użytkownika**
   W celu zapewnienia kontroli nad kontami użytkowników i uprawnieniami dostępu, organizacja powinna zapewnić wdrożenie odpowiedniej polityki, gdzie dostęp do zasobów jest przydzielany na podstawie pełnionej funkcji i roli,

6) **Ochrona przed złośliwym oprogramowaniem**
   W celu ograniczenia możliwości korzystania z niezaufanego oprogramowania, organizacja powinna zapewnić mechanizmy ochrony przed złośliwym oprogramowaniem na wszystkich urządzeniach,

7) **Zabezpieczenia dodatkowe**
   W celu zabezpieczenia przed utratą danych organizacja powinna:
   - tworzyć kopie zapasowe danych i zapisywać je regularnie na innym urządzeniu lub w pamięci masowej w chmurze (online),
   - stosować podejście „Zero trust" – zero zaufania. Każde żądanie dostępu do systemu powinno być weryfikowane na podstawie polityki uwierzytelniania i autoryzacji,

8) **Usługi cyfrowe i identyfikacja w sieci**
   W celu bezpiecznego dostępu do usług cyfrowych organizacja powinna wykorzystywać odpowiednie mechanizmy identyfikacji i ochrony danych użytkownika.

Zasadniczym dokumentem, będącym podstawą do przeprowadzenia procesu certyfikacji przez jednostkę certyfikującą jest sporządzany przez certyfikatora Raport z oceny.

4.1.4 Przegląd

Jednostka certyfikująca dokonuje przeglądu dokumentacji zebranej w trakcie certyfikacji.

Przegląd wszystkich informacji i wyników dotyczących oceny pod względem merytorycznym i formalnym ma na celu dostarczenie dowodów zgodności procesu podlegającego certyfikacji z przyjętymi wymaganiami dokumentów stanowiących kryteria oceny.

4.1.5 Decyzja i wydanie/odmowa wydania certyfikatu

Po dokonaniu przeglądu wyników procesu certyfikacji podejmowana jest decyzja o wydaniu lub odmowie wydania certyfikatu. Maksymalny czas na wydanie decyzji w sprawie certyfikacji wynosi 60 dni od daty podpisania umowy o certyfikację.

W przypadku pozytywnego zakończenia procesu wystawiany jest certyfikat. Decyzja o odmowie wydania certyfikatu przekazywana jest klientowi pisemnie wraz z uzasadnieniem. W przypadku wydania decyzji odmownej klient ma prawo w ciągu 14 dni od doręczenia decyzji złożyć odwołanie do jednostki certyfikującej co do jej treści wraz z uzasadnieniem.

Certyfikat przyznawany jest na okres 1 roku, z wyjątkiem wprowadzenia zmian w warunkach przyznawania certyfikatów, nieprzestrzegania warunków korzystania z certyfikatu lub wyraźnej rezygnacji z certyfikacji wyrażonej przez klienta.

Certyfikat zgodności zawierać będzie informacje, które identyfikują:

a) nazwę i adres jednostki certyfikującej,
b) datę wydania certyfikatu,
c) nazwę i adres klienta,
d) zakres certyfikacji,
e) dokumenty odniesienia,
f) nazwę i akronim programu certyfikacji,
g) datę ważności certyfikatu,
h) podpis osoby upoważnionej do wydania certyfikatu.

4.1.5.1 Utrzymanie certyfikatu

NASK – PIB jest właścicielem certyfikatu i monitoruje na bieżąco jego wykorzystanie poprzez analizę informacji z rynku dotyczących jego stosowania oraz rejestrację wszelkich technicznych i handlowych informacji odnoszących się do wydanego certyfikatu.

Jej celem jest sprawdzenie, czy podmiot otrzymujący certyfikację nadal spełnia wymagania określone w programie certyfikacji, a środowisko przedsiębiorstwa nie uległo zmianie w wyniku zmian organizacyjnych lub technologicznych, pojawieniu się nowych zagrożeń cyberbezpieczeństwa, analizy ryzyka lub dokumentacji przyjętej w zakresie stosowania niniejszego programu oraz prawidłowo wykorzystuje symbol certyfikacji.

Przegląd ważności certyfikatu może spowodować zawieszenie, ograniczenie lub cofnięcie certyfikatu przez jednostkę certyfikującą.

4.1.5.2 Zawieszenie, zakończenie, rozszerzenie i cofnięcie certyfikatu

Zawieszenie certyfikatu może nastąpić na wniosek klienta lub w przypadku:

a) stwierdzenia niezgodności w sposobie wykorzystywania lub powoływania się na wydany certyfikat,
b) braku lub nieskutecznej realizacji przez klienta działań wynikających ze zmiany wymagań certyfikacyjnych,
c) niewywiązywania się przez klienta z warunków zawartych w umowie o certyfikację.

Maksymalny okres zawieszenia certyfikatu nie może przekraczać 3 miesięcy. Warunki przywrócenia udzielonej certyfikacji są przedstawiane klientowi przez NASK - PIB na piśmie. Wznowienie certyfikacji odbywa się na wniosek klienta i poprzez ocenę spełnienia warunków przywrócenia.

Cofnięcie certyfikatu następuje w przypadku nieusunięcia w terminie warunków przywrócenia certyfikacji lub na wniosek klienta. Zakończenie następuje z dniem obowiązywania określonym w certyfikacie.

W przypadku otrzymania decyzji o cofnięciu lub bez oddzielnego powiadomienia w przypadku zakończenia certyfikacji klient zobowiązany jest do zaprzestania powoływania się na wydany certyfikat.

Stosownie do wyżej wymienionych działań uaktualniany jest wykaz certyfikatów. W wykazie znajduje się zapis o zawieszonym certyfikacie lub w przypadku cofnięcia - certyfikat zostaje usunięty z wykazu.

4.1.5.3 Przedłużenie ważności i zmiany mające wpływ na certyfikację

Przedłużenie ważności certyfikatu wymaga złożenia wniosku wraz z kompletną dokumentacją co najmniej 1 miesiąc przed terminem upływu jego ważności. Jednostka certyfikująca prowadzi w tym zakresie działania określone w pkt. 4 niniejszego dokumentu.

Przeniesienie certyfikacji może nastąpić w przypadku:

a) zmiany nazwy lub/i adresu klienta,
b) zmiany statusu prawnego klienta.

Proces ten prowadzony jest na pisemny wniosek klienta. Jednostka certyfikująca określa zakres wymaganej dokumentacji, która powinna być dołączona do wniosku uwzględniając zakres i rodzaj wnioskowanych zmian.

Certyfikat podlegający zmianie zostaje unieważniony a w jego miejsce wydaje się nowy z zastrzeżeniem, że termin ważności nowego certyfikatu biegnie od dnia wystąpienia przyczyny dokonanej zmiany do dnia pierwotnego końca ważności certyfikatu unieważnionego.

W przypadku wystąpienia zmiany wymagań stanowiących podstawę certyfikacji jednostka certyfikująca przekazuje klientowi informację o zakresie zmian oraz o terminie ich wdrożenia w celu utrzymania ważności certyfikatu, który zostanie wydany.

Zmiany mające wpływ na certyfikację mogą wynikać z informacji uzyskanych przez jednostkę certyfikującą już po rozpoczęciu certyfikacji.

Jeśli będzie to konieczne, działania wdrażania zmian mogą obejmować w szczególności ocenę, przegląd, decyzję w sprawie certyfikacji oraz wydanie zmienionych dokumentów certyfikacyjnych.

Jednostka certyfikująca przedstawia klientowi sposób weryfikacji wdrożenia wymagań. W przypadku niespełnienia przez klienta określonych wymogów NASK – PIB zawiesza wydany certyfikat.

5. Poufność

NASK – PIB zobowiązuje się do zachowania poufności wszystkich informacji uzyskanych od klientów w procesie certyfikacji. Usługi na każdym etapie są świadczone w sposób bezstronny, obiektywny i etyczny. Personel własny oraz podwykonawcy zostali zobowiązani do zachowania zasad poufności w zakresie wszystkich informacji uzyskanych w procesie certyfikacji.

Jeżeli NASK – PIB jest zobowiązany poprzez odpowiednie przepisy prawne do ujawniania informacji poufnej, to klient zostanie o tym poinformowany, o ile nie jest to zabronione w trybie przepisów szczególnych.

6. Skargi i odwołania

Klient ma prawo odwołać się od decyzji w sprawie certyfikacji (pkt 4.1.5) lub złożyć skargę do jednostki certyfikującej.

Odwołania i skargi są rozpatrywane przez NASK – PIB z zachowaniem zasady bezstronności oraz rzetelności.

Odwołanie powinno być wniesione do Dyrektora NASK-PIB w terminie do 14 dni od daty otrzymania decyzji, z którą klient się nie zgadza.

Klient lub inna zainteresowana strona ma prawo złożyć skargę dotyczącą funkcjonowania jednostki certyfikującej. Skarga może być wniesiona w dowolnej formie do Kierownika Jednostki Certyfikującej NASK-PIB.

Tryb wnoszenia skargi lub odwołania jest opisany procedurą postępowania, wskazaną na stronie internetowej programu Firma Bezpieczna Cyfrowo.

7. Opłaty

Klient jest zobowiązany pokryć koszty certyfikacji zgodnie z zawartą umową, niezależnie od jej wyników. Opłaty za certyfikację są określone w cenniku (regulaminie opłat) umieszczonym na stronie internetowej programu Firma Bezpieczna Cyfrowo.

8. Wykaz certyfikatów

NASK-PIB prowadzi wykaz wydanych certyfikatów. Wykaz ten zawiera w szczególności: identyfikację klienta, oznaczenie procesu, termin ważności certyfikatu oraz oznaczenie dokumentu normatywnego, na zgodność z którym była przeprowadzona certyfikacja.

Informacje powyższe są dostępne na stronie internetowej programu Firma Bezpieczna Cyfrowo.

9. Informacje uzupełniające

Wniosek o certyfikację oraz dokumenty wymienione w pkt. 3.1 i pkt. 3.2 stanowią integralną część niniejszego programu.

Uzyskany przez klienta certyfikat nie zwalnia go z odpowiedzialności za przebieg procesu zarządzania cyberbezpieczeństwem w przedsiębiorstwie i nie może powodować przeniesienia części tej odpowiedzialności na jednostkę certyfikującą.

Załącznik nr 1

Proces wdrażania odpowiednich środków technicznych i organizacyjnych składających się na cyberbezpieczeństwo w MŚP.

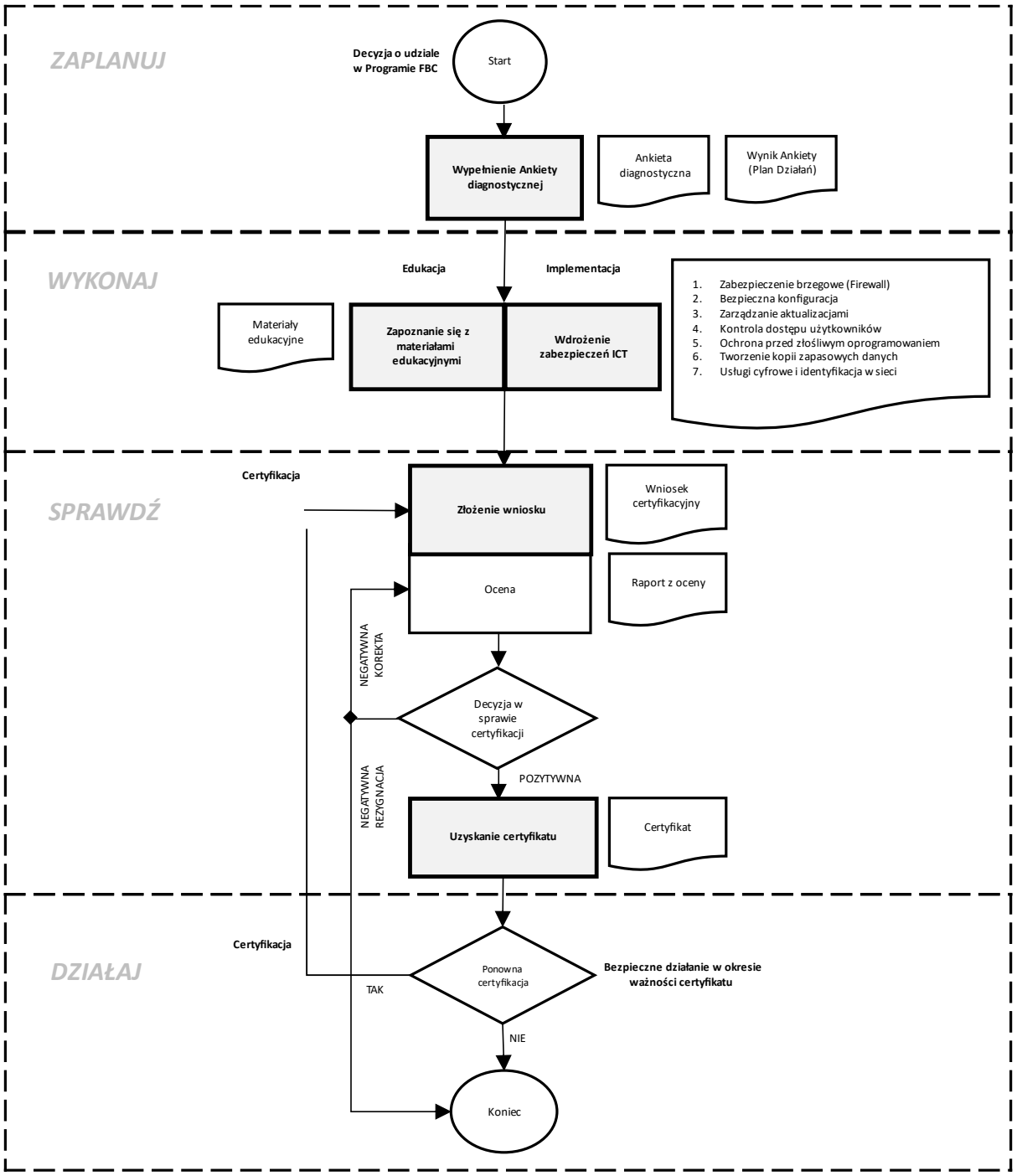

Diagram 1