Certyfikacja NASK

PC-FBC
Program certyfikacji
Firma Bezpieczna Cyfrowo

(Egzemplarz dla Klienta)

Wersja **1.4.1** (data wydania 23.07.2024)

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 certyfikacji jest określenie zasad przebiegu certyfikacji procesu zarządzania cyberbezpieczeństwem[2] w małych i średnich przedsiębiorstwach (MŚP) poprzez niezależną ocenę zgodności z wymaganiami określonymi przez jednostkę certyfikującą i zgodnie z przyjętą w programie metodyką oceny.

Program certyfikacji ma zapewnić, że proces zarządzania cyberbezpieczeństwa w firmach przystępujących do programu jest oceniony i atestowany na zgodność z wyspecyfikowanymi wymaganiami przez niezależną stronę trzecią (tj. Jednostkę Certyfikującą).

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 https://certyfikacja.nask.pl.

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

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

Zakłada się, że przedsiębiorstwo, które uzyskało certyfikat FBC, wdrożyło dobre praktyki i spełnia podstawowe wymagania z obszaru zarządzania cyberbezpieczeństwem. W szczególności:

- utworzyło i aktualizuje rejestr aktywów;
- wdrożyło i prowadzi politykę dostępu i bezpiecznych haseł;
- wdrożyło wymagane przez program certyfikacji zabezpieczenia techniczne przed cyberzagrożeniami i atakami z internetu;
- wprowadziło politykę tworzenia kopii zapasowych;
- prawidłowo wykorzystuje środki identyfikacji elektronicznej oraz bezpiecznie korzysta z usług cyfrowych.

[2] Patrz Załącznik 1: Proces wdrażania odpowiednich środków technicznych i organizacyjnych składających się na cyberbezpieczeństwo w MŚP (w skrócie: proces zarządzania cyberbezpieczeństwem).

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[3].

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.

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:

[3] Do udziału w pilotażu programu certyfikacji kwalifikowane są wyłącznie MŚP mające siedzibę w Polsce (osoba prawna) lub miejsce zamieszkania w Polsce (osoba fizyczna).

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 – proces wdrażania odpowiednich środków technicznych i organizacyjnych składających się na cyberbezpieczeństwo w MŚP, o którego certyfikację klient wnioskuje (w skrócie: proces zarządzania cyberbezpieczeństwem),

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.

4. Wymagania certyfikacyjne i metodyka oceny

4.1. Wymagania certyfikacyjne

Wymagania certyfikacyjne w niniejszym programie określają:

1) PC-FBC Program certyfikacji Firma Bezpieczna Cyfrowo,
2) ST1 - Specyfikacja techniczna - Wymagania dla Programu certyfikacji Firma Bezpieczna Cyfrowo.

4.2. Metodyka oceny

Metodykę oceny stanowi dokument M1 - Metodyka oceny dla Programu certyfikacji Firma Bezpieczna Cyfrowo.

5. Przebieg procesu certyfikacji

5.1. Etapy procesu certyfikacji Firma Bezpieczna Cyfrowo

5.1.1. Wniosek o certyfikację

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

Formularz wniosku wraz ze wszystkimi wymaganymi wzorami oświadczeń dostępny jest na stronie internetowej Programu certyfikacji Firma Bezpieczna Cyfrowo oraz w Jednostce Certyfikującej.

Klient może otrzymać na życzenie informacje o szczegółach procedury certyfikacji w ramach Programu certyfikacji 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 akceptacją 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.

5.1.2. 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 certyfikacji 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 certyfikacji 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.

5.1.3. Ocena

Przedmiotem oceny jest proces wdrażania środków technicznych i organizacyjnych składających się na cyberbezpieczeństwo w MŚP: od wypełnienie ankiety diagnostycznej i zapoznania z materiałami edukacyjnymi dostępnymi na stronie internetowej „Firma Bezpieczna Cyfrowo" poprzez zapoznanie się ze specyfikacją wymagań dla Programu certyfikacji Firma Bezpieczna Cyfrowo, implementację odpowiednich środków technicznych i organizacyjnych zapewniających spełnienie podstawowych wymagań z obszaru zarządzania cyberbezpieczeństwem, 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 spełnienie wymagań w obszarze zarządzania procesem cyberbezpieczeństwa, w zakresie następujących środków organizacyjnych i technicznych służących zapewnieniu cyberbezpieczeństwa:

Zakres oceny

W celu określenia obszaru podlegającego ocenie organizacja powinna zidentyfikować zakres objęty procesem wdrażania środków technicznych i organizacyjnych składających się na cyberbezpieczeństwo całej lub dobrze zdefiniowanej części organizacji, zidentyfikować aktywa oraz usługi stron trzecich objęte tym procesem.

Zabezpieczenie brzegowe (Firewall)

W celu zapewnienia bezpieczeństwa usług dostępnych z Internetu organizacja powinna zapewnić bezpieczeństwo każdego urządzenia w sieci firmy za pomocą prawidłowo skonfigurowanego i umiejscowionego w miejscu styku sieci organizacji z Internetem, firewalla, chroniącego zasoby sieciowe.

Bezpieczna konfiguracja

W celu zapewnienia właściwego poziomu bezpieczeństwa informacji, organizacja powinna wdrożyć zarządzanie odpowiednią konfiguracją systemów informacyjnych, sprzętu biurowego oraz urządzeń sieciowych.

Zarządzanie aktualizacjami

W celu zapewnienia bezpiecznego korzystania z urządzeń i instalowanego na nich oprogramowania, organizacja powinna zapewnić, że całe wykorzystywane oprogramowanie jest aktualizowane.

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.

Ochrona przed złośliwym oprogramowaniem

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

Tworzenie kopii zapasowych danych

W celu zabezpieczenia przed utratą danych organizacja powinna:

- tworzyć kopie zapasowych 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.

Usługi cyfrowe i identyfikacja elektroniczna

W celu bezpiecznego dostępu do usług cyfrowych organizacja powinna wykorzystywać odpowiednie mechanizmy identyfikacji elektronicznej i ochrony danych użytkownika.

5.1.3.1. Przebieg oceny

Zasadniczym dokumentem, będącym podstawą do przeprowadzenia procesu certyfikacji przez Jednostkę Certyfikującą jest sporządzany przez klienta kwestionariusz oceny. Jednostka Certyfikująca prowadzi weryfikację i ocenę kwestionariusza i oświadczeń złożonych przez klienta, poprzez niezależną ocenę zgodności z wymaganiami określonymi przez jednostkę certyfikującą zgodnie z przyjętą w programie metodyką oceny. Wynik tej oceny, ujęty jest w Raporcie z oceny.

W zakresie pozyskiwania dowodów na spełnienie lub celem weryfikacji wymagań, Jednostka Certyfikująca może zdecydować o konieczności przeprowadzenia inspekcji i testów za pomocą środków komunikacji elektronicznej na odległość.

5.1.4. 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.

5.1.5. 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 30 dni od daty podpisania umowy o certyfikację pod warunkiem uiszczenia opłaty certyfikacyjnej i doręczenia Jednostce Certyfikującej poprawnie i kompletnie wypełnionego kwestionariusza.

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 adresu klienta,
d) zakres certyfikacji,
e) dokumenty odniesienia,
f) nazwę i akronim programu certyfikacji,
g) datę ważności certyfikatu,
h) podpis osoby upoważnionej do wydania certyfikatu.

5.1.5.1. 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.

5.1.5.2. 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 zakończeniu 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.

5.1.5.3. 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.

Działanie to prowadzone 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.

6. 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.

7. 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 certyfikacji Firma Bezpieczna Cyfrowo.

8. 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 certyfikacji Firma Bezpieczna Cyfrowo.

9. 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 certyfikacji Firma Bezpieczna Cyfrowo.

10. 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[4] procesu zarządzania cyberbezpieczeństwem w przedsiębiorstwie i nie może powodować przeniesienia części tej odpowiedzialności na Jednostkę Certyfikującą.

[4] Planowanie działań, wdrożenie, realizacja i utrzymanie.

Załącznik nr 1

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

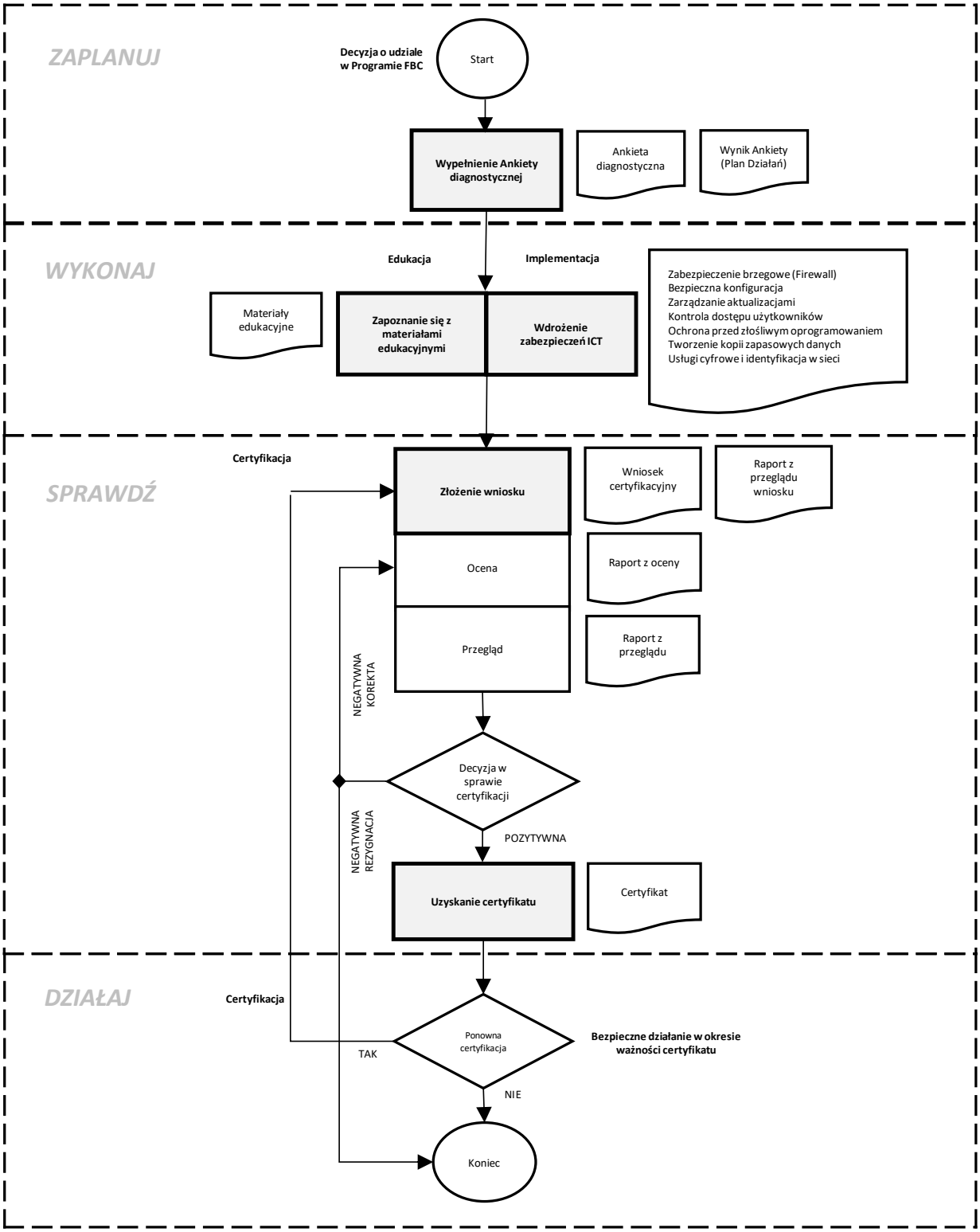

Diagram 1