Załącznik
do Zarządzenia nr 10
Rektora Uniwersytetu w Białymstoku
z dnia 6 lutego 2020 r.

PROGRAM KURSU DOKSZTAŁCAJĄCEGO

I. INFORMACJE OGÓLNE

1. Nazwa kursu dokształcającego:
   Zarządzanie usługami IT oraz Systemem Zarządzania Bezpieczeństwem Informacji
2. Nazwa jednostki prowadzącej kurs dokształcający:
   Wydział Ekonomii i Finansów
3. Czas trwania kursu dokształcającego:
   Moduł I – 5 dni x 10 godz. dydaktycznych = 50 godz.
   Moduł II – 5 dni x 10 godz. dydaktycznych = 50 godz.
   Moduł III – 2 dni x 10 godz. dydaktycznych = 20 godz.
   Moduł IV – 5 dni x 10 godz. dydaktycznych = 50 godz.
   Moduł V – 5 dni x 10 godz. dydaktycznych = 50 godz.
   - łącznie 220 godz. zajęć teoretycznych i warsztatowych,
   - zajęcia realizowane w systemie weekendy + dni pracujące,
   - zamknięcie kursu do 31 maja 2020 r.
4. Założenia i cele ogólne:
   Założeniem kursu dokształcającego *Zarządzanie usługami IT oraz Systemem Zarządzania Bezpieczeństwem Informacji* jest przekazanie uczestnikom najaktualniejszej wiedzy oraz wyposażenie ich w praktyczne umiejętności, z obszarów bezpośrednio związanych z działaniem przedsiębiorstw i podmiotów sektora publicznego, ustrukturyzowanych w pięciu modułach dotyczących systemu zarządzania bezpieczeństwem informacji, usług IT, audytu, ciągłości działania, przetwarzania danych osobowych w chmurze, kontroli zarządczej. W ramach kursu uczestnicy będą mogli również uzyskać niezależny międzynarodowy certyfikat Auditora Wiodącego Systemu Zarządzania Ciągłością Działania ISO 22301 (Akredytacja IRCA 17456).
5. Program kursu dokształcającego zaopiniowany na posiedzeniu Rady Wydziału Ekonomii i Finansów w dniu 13 stycznia 2020 r.

II. ZAKŁADANE EFEKTY UCZENIA SIĘ

Po ukończeniu kursu dokształcającego:

1) w zakresie wiedzy, absolwent zna i rozumie:
   – pojęcie audytu, SZBI, ciągłości działania, chmury, kontroli zarządczej,
   – elementy modelowego systemu zarządzania bezpieczeństwem informacji w organizacji,
   – narzędzia i metody wykonywania audytów oraz kontroli zarządczej,

– aktualne normy ISO i obowiązujące regulacje prawne z zakresu bezpieczeństwa informacji,
– etapy i zasady planowania audytu i jego realizacji,
– zakres zadań i kompetencji audytora i inspektora ochrony danych,
– zakres stosowania i zapisy norm ISO/IEC 20000-1:2011, ISO 19011:2018, ISO 22301, ISO/IEC 27017,
– podstawy systemu zarządzania usługami informatycznymi,
– metody tworzenia i zarządzania programem audytu i kontroli zarządczej,
– techniki opracowania składania raportów o wynikach nadzoru,
– podstawową terminologię wynikającą z norm ISO, nauk o zarządzaniu, ekonomiczną, prawniczą i informatyczną dotyczącą obszaru bezpieczeństwa informacji, ciągłości działania, chmury,
– podstawy m.in. prawne i finansowe funkcjonowania jednostek sektora publicznego i prywatnego oraz podstawy zarządzania w tych jednostkach,
– procesy zachodzące w organizacji wymagające zaangażowania audytora i inspektora ochrony danych,
– funkcjonowanie systemów informatycznych i usług IT w jednostkach administracji publicznej i podmiotach sektora prywatnego,
– wytyczne dotyczące stosowania zabezpieczeń, w tym zabezpieczeń specyficznych dla przetwarzania w chmurze,
– rozpoznanie i wybór odpowiednich zabezpieczeń ISO/IEC 27017:2015 w celu zarządzania ryzykiem związanym z usługami w chmurze,
– istotę zachowań etycznych i nieetycznych w pracy audytora i inspektora ochrony danych,
– sposoby niezależnego audytu systemu zarządzania ciągłości biznesowej i systemu zarządzania usługami IT oraz kontroli zarządczej,

2) w zakresie umiejętności, absolwent potrafi:
– reagować na typowe zagrożenia dotyczące bezpieczeństwa informacji i związanych z usługami w chmurze,
– interpretować wymagania normy ISO/IEC 20000-1:2011, ISO 22301 w kontekście audytu,
– nadzorować, tworzyć i gromadzić dokumentację z audytu wymaganą przepisami prawa i norm ISO,
– stosować najistotniejsze zapisy normy ISO 27001, ISO/IEC 27017,
– kierować audytem systemu zarządzania ciągłości działania i systemu zarządzania usługami informatycznymi,
– dokonywać wyboru zabezpieczeń ISO/IEC 27017:2015, odpowiadających wynikom oceny ryzyka,
– prowadzić audyt i kontrolę zarządczą samodzielnie lub we współpracy z zespołem audytowym,
– planować, przeprowadzać i analizować rozmowy z podmiotami audytowanymi,

– opracować rekomendacje dla organizacji mające na celu podniesienie poziomu zarządzania bezpieczeństwem informacji i ciągłości działania,
– rozróżnić etyczne i nieetyczne zachowania w stosunkach w organizacji mające związek z prowadzeniem audytu i kontroli zarządczej,
– rozwijać umiejętność pracy analitycznej i koncepcyjnej, samodzielnie lub w zespole audytowym,
– zaplanować własne działania w celu wykonania obowiązków audytora i inspektora ochrony danych,
– prowadzić szkolenia wewnętrzne w zakresie SZBI dla personelu organizacji,
– skutecznie motywować siebie i innych do zdobywania wiedzy,

3) w zakresie kompetencji społecznych, absolwent jest gotów do:
– pokonywania problemów i trudności wynikających z kontaktów interpersonalnych i hierarchii w organizacji,
– własnego wpływu na organizację poprzez kontrolę zarządczą, kształtowanie i poprawę funkcjonalności usług IT, ciągłości działania, systemu zarządzania bezpieczeństwem informacji,
– samodoskonalenia, podnoszenia własnych kompetencji ważnych w relacjach interpersonalnych i funkcjonowaniu organizacji skutecznego motywowania współpracowników w zespole audytowym,
– zarządzania z sukcesem komunikatami i wywiadami odnośnie audytu i kontroli zarządczej,
– podnoszenia poziom umiejętności budowania relacji interpersonalnych,
– stosowania Kodeksu Praktyki Zarządzania Ciągłością Działania i Kodeksu Postępowania ISO/IEC 20000-2,
– pracy w zespole, przyjmując w nim różne role,
– doskonalenia skutecznych metod komunikacji i negocjacji w wykonywaniu zadań audytora i inspektora ochrony danych.

Informację o uzyskanych efektach uczenia się uczestnicy otrzymają wraz ze świadectwem ukończenia kursu dokształcającego.
Nabyta w trakcie kursu dokształcającego wiedza, umiejętności i kompetencje społeczne mają istotną wagę w działalności zawodowej inspektora ochrony danych oraz audytora.

Kryteria weryfikacji osiągnięcia poszczególnych efektów uczenia się:
Weryfikacja odbywa się na podstawie aktywności uczestnika, prac samodzielnych i grupowych, wyników zajęć warsztatowych, egzaminu końcowego.

III. WYKAZ ZAJĘĆ I LICZBA GODZIN DYDAKTYCZNYCH

Nazwa zajęć/ modułów	Liczba godzin dydaktycznych
1. Auditor Wiodący systemu zarządzania usługami IT wg ISO/IEC 20000:2018	50 godzin
2. Auditor Wiodący Systemu Zarządzania Ciągłością Działania ISO 22301	50 godzin
3. Bezpieczeństwo Informacji w chmurze wg ISO/IEC 27017 z elementami ochrony danych osobowych przetwarzanych w chmurze (ISO/IEC 27018)	20 godzin
4. Auditor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji wg ISO/IEC 27001:2017	50 godzin
5. Koordynator kontroli zarządczej w administracji publicznej	50 godzin

IV. WARUNKI UKOŃCZENIA KURSU DOKSZTAŁCAJĄCEGO:

1. Obecność na co najmniej 80 % zajęć z każdego modułu.
2. Zaliczenie wszystkich zajęć przewidzianych programem kursu dokształcającego.