Możliwość dofinansowania

CISM - Certified Information Security Manager

Numer usługi 2024/05/07/52766/2142115

5 079,90 PLN brutto
4 130,00 PLN netto
181,43 PLN brutto/h
147,50 PLN netto/h

NOBLEPROG POLSKA Spółka z o.o

★★★★☆

zdalna w czasie rzeczywistym
Usługa szkoleniowa
28 h
03.09.2024 do 06.09.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Administracja IT i systemy komputerowe
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Odbiorcami szkolenia mogą być specjaliści ds. Bezpieczeństwa z 3-5-letnim doświadczeniem w branży Menedżerowie bezpieczeństwa informacji lub osoby odpowiedzialne za zarządzanie; Pracownicy ds. Bezpieczeństwa informacji, dostawcy usług bezpieczeństwa informacji, którzy wymagają dogłębnego zrozumienia zarządzania bezpieczeństwem informacji, w tym: CISO, CIO, CSO, urzędnicy ds. Prywatności, menedżerowie ryzyka, audytorzy bezpieczeństwa i pracownicy ds. Zgodności, personel BCP / DR, kierownictwo wykonawcze i operacyjne odpowiedzialne za funkcje zabezpieczające oraz osoby które zamierzają podnieść swoje kompetencje w tym zakresie .
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	30-08-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	28
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Zaznajomienie uczestników z pojęciami związanymi z bezpieczeństwem informacji;
Przygotowanie do certyfikacji CISM

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
uczestnik prawidłowo przeprowadza 1. Nadzór nad bezpieczeństwem informacji 2. Zarządzanie ryzykiem i zgodnością przetwarzania informacji	ocena pracy i wykonywanych ćwiczeń podczas szkolenia	Test teoretyczny
uczestnik tworzy procesury i zarządza nimi - w odniesieniu do bezpieczeństwa informacji	ocena pracy i wykonywanych ćwiczeń podczas szkolenia	Test teoretyczny
uczestnik samodzielnie zarządza Incydentem bezpieczeństwa informacji	ocena pracy i wykonywanych ćwiczeń podczas szkolenia	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

zaświadczenie z opisem efektów uczenia się

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

zaświadczenie z informacją

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

zaświadczenie z informacją

Program

Domain 1—Information Security Governance

Establish and maintain an information security governance framework and supporting processes to ensure that the information security strategy is aligned with organizational goals and objectives, information risk is managed appropriately and program resources are managed responsibly.

- 1.1 Establish and maintain an information security strategy in alignment with organizational goals and objectives to guide the establishment and ongoing management of the information security program.
- 1.2 Establish and maintain an information security governance framework to guide activities that support the information security strategy.
- 1.3 Integrate information security governance into corporate governance to ensure that organizational goals and objectives are supported by the information security program.
- 1.4 Establish and maintain information security policies to communicate management's directives and guide the development of standards, procedures and guidelines.
- 1.5 Develop business cases to support investments in information security.
- 1.6 Identify internal and external influences to the organization (for example, technology, business environment, risk tolerance, geographic location, legal and regulatory requirements) to ensure that these factors are addressed by the information security strategy.
- 1.7 Obtain commitment from senior management and support from other stakeholders to maximize the probability of successful implementation of the information security strategy.
- 1.8 Define and communicate the roles and responsibilities of information security throughout the organization to establish clear accountabilities and lines of authority.
- 1.9 Establish, monitor, evaluate, and report metrics (for example, key goal indicators [KGIs], key performance indicators [KPIs], key risk indicators [KRIs]) to provide management with accurate information regarding the effectiveness of the information security strategy.

Domain 2—Information Risk Management and Compliance

Manage information risk to an acceptable level to meet the business and compliance requirements of the organization.

- 2.1 Establish and maintain a process for information asset identification and classification to ensure that measures taken to protect assets are proportional to their business value.
- 2.2 Identify legal, regulatory, organizational and other applicable requirements to manage the risk of noncompliance to acceptable levels.
- 2.3 Ensure that risk assessments, vulnerability assessments and threat analyses are conducted periodically and consistently to identify risk to the organization's information.
- 2.4 Determine and implement appropriate risk treatment options to manage risk to acceptable levels.
- 2.5 Evaluate information security controls to determine whether they are appropriate and effectively mitigate risk to an acceptable level.
- 2.6 Integrate information risk management into business and IT processes (for example, development, procurement, project management, mergers and acquisitions) to promote a consistent and comprehensive information risk management process across the organization.
- 2.7 Monitor existing risk to ensure that changes are identified and managed appropriately.
- 2.8 Report noncompliance and other changes in information risk to appropriate management to assist in the risk management decision-making process.

Domain 3—Information Security Program Development and Management

Establish and manage the information security program in alignment with the information security strategy.

- 3.1 Establish and maintain the information security program in alignment with the information security strategy.
- 3.2 Ensure alignment between the information security program and other business functions (for example, human resources [HR], accounting, procurement and IT) to support integration with business processes.
- 3.3 Identify, acquire, manage, and define requirements for internal and external resources to execute the information security program.
- 3.4 Establish and maintain information security architectures (people, process, technology) to execute the information security program.
- 3.5 Establish, communicate, and maintain organizational information security standards, procedures, guidelines and other documentation to support and guide compliance with information security policies.
- 3.6 Establish and maintain a program for information security awareness and training to promote a secure environment and an effective security culture.
- 3.7 Integrate information security requirements into organizational processes (for example, change control, mergers and acquisitions, development, business continuity, disaster recovery) to maintain the organization's security baseline.
- 3.8 Integrate information security requirements into contracts and activities of third parties (for example, joint ventures, outsourced providers, business partners, customers) to maintain the organization's security baseline.
- 3.9 Establish, monitor, and periodically report program management and operational metrics to evaluate the effectiveness and efficiency of the information security program.

Domain 4—Information Security Incident Management

Plan, establish and manage the capability to detect, investigate, respond to and recover from information security incidents to minimize business impact.

- 4.1 Establish and maintain an information security incident classification and categorization process to allow accurate identification of and response to incidents.
- 4.2 Establish, maintain, and align incident response plan with the business continuity plan and disaster recovery plan to ensure an effective and timely response to information security incidents.
- 4.3 Develop and implement processes to ensure the timely identification of information security incidents.
- 4.4 Establish and maintain processes to investigate and document information security incidents to be able to respond appropriately and determine their causes while adhering to legal, regulatory and organizational requirements.
- 4.5 Establish and maintain incident handling processes to ensure that the appropriate stakeholders are involved in incident response management.
- 4.6 Organize, train and equip teams to effectively respond to information security incidents in a timely manner.
- 4.7 Test and review the incident management plans periodically to ensure an effective response to information security incidents and to improve response capabilities.
- 4.8 Establish and maintain communication plans and processes to manage communication with internal and external entities.
- 4.9 Conduct post-incident reviews to determine the root cause of information security incidents, develop corrective actions, reassess risk, evaluate response effectiveness and take appropriate remedial actions.
- 4.10 Establish and maintain integration among the incident response plan, disaster recovery plan and business continuity plan.

Harmonogram

Liczba przedmiotów/zajęć: 0

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 079,90 PLN
Koszt przypadający na 1 uczestnika netto	4 130,00 PLN
Koszt osobogodziny brutto	181,43 PLN
Koszt osobogodziny netto	147,50 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Filip Stachecki

Wykształcenie wyższe,
Doświadczenie zawodowe jako trener i szkoleniowiec,
Przeprowadził ponad 300 godzin szkoleniowych z zakresu m.in.
UML and OMG Certified UML Professional, C#, Visual Basic, Visual Basic .NET, VBA, Delphi, SQL, ASP, UML, HTML, CSS, XML, XSL, .NET, Web Services,
Posiada certyfikaty i akredytacje z zakresu OMG Certified UML Professional Advanced OMG Certified UML Professional Intermediate
OMG Certified UML Professional Fundamental
OMG Certified Systems Modeling Professional - Model User
OMG Certified Expert in BPM 2

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymają materiały szkoleniowe w wersji elektronicznej - w formie ćwiczeń, skryptów.

Warunki uczestnictwa

Znajomość języka angielskiego w stopniu komunikatywnym

Informacje dodatkowe

Kontakt w sprawie szkolenia, dotyczące kwestii organizacyjnych :

Monika Fengler monika.fengler@nobleprog.pl

Kontakt w sprawie dofinansowania do szkolenia :

Patrycja Foremniak patrycja.foremniak@nobleprog.com , tel. 694 117 999

Przerwy będą ustalane między prowadzącym i uczestnikami na bieżąco, wg potrzeby.

Szkolenie może być zwolnione z VAT na podstawie **art. 43 ust. 1 ustawy o VAT – w przypadku dofinansowania, które wynosi co najmniej 70% ceny netto szkolenia.**

Proszę przy zapisie o podanie wysokości dofinansowania oraz nazwę Operatora regionalnego, który udzielił dofinansowania.

Warunki techniczne

Wymagane:

- wymagania sieciowe, oprogramowanie **- komputer ze stabilnym podłączeniem do Internetu (min 10Mbit/s download i 1Mbit/s upload);**
- **przeglądarka internetowa** Chrome lub Firefox;
- wymagania w sprzęt - dobrej jakości **mikrofon lub słuchawki;**
- rodzaj komunikatora- Szkolenie odbędzie się na platformie ZOOM

Minimalne wymagania sprzętowe:

Procesor jednordzeniowy o taktowaniu co najmniej 1Ghz,

Pamięć RAM – zalecana 4Gb,

w laptopach posiadających jeden lub dwa rdzenie liczba klatek na sekundę jest ograniczona podczas udostępniania ekranu (około 5 klatek na sekundę). Aby uzyskać optymalne wyniki podczas udostępniania ekranu z laptopów, zalecamy wykorzystanie procesora posiadającego cztery procesory lub więcej,

System Linux wymaga procesora lub karty graficznej z obsługą sterownika OpenGL 2.0 lub nowszej wersji.

- **Uczestnik otrzyma link do szkolenia na 2 dni przed rozpoczęciem usługi**
- **Link będzie ważny przez cały okres trwania usługi**

Kontakt

Patrycja Foremniak

E-mail patrycja.foremniak@nobleprog.com
Telefon (+48) 694 117 999