CISA – Certified Information Systems Auditor

Дати проведення: 8-12 листопада 2021
Місце проведення: ISSP Training Center, м. Київ, вул. Радищева 10/14
Тривалість: 5 днів з 10:00 до 18:00 з перервами на обід та кава-паузи
Мова викладання: українська / російська
Навчальний комплект включає в себе:
- офіційні навчальні матеріали в електронному вигляді від ISACA – англійською мовою;
- ваучер для складання іспиту

Вимоги до учасників:
- знання англійської мови на рівні не нижче intermediate (всі навчальні матеріали надаються англійською)

ДЛЯ КОГО

- Професіонали, які готуються стати сертифікованими CISA
- Фінансові аудитори, які переходять на IT-аудит
- IT-спеціалісти, які переходять на IT-аудит
- Фахівці Middle рівня, які змінюють кар'єру

ДАНИЙ КУРС ДОПОМОЖЕ

Отримати краще розуміння проведення аудиту ІБ та керівних принципів і стандартів ІБ
Розвивати практичні знання з п'яти доменів CISA.

ПРОГРАМА КУРСУ

Домен 1 - Процес аудиту інформаційної системи

1. Планування аудиту, щоб визначити захищеність та контрольовані інформаційні системи, та чи забезпечують вони цінність для організації.
2. Проведення аудиту відповідно до стандартів аудиту ІБ та стратегії аудиту ІБ на основі ризиків.
3. Комунікації з зацікавленими сторонами про прогрес аудиту, висновки, результати та рекомендації.
4. Проведення контролю аудиту, з метою оцінки якості опрацювання ризиків.
5. Оцінювання управління IT та моніторинг контролів.
6. Використання інструментів аналізу даних з метою спрощення процесів аудиту.
7. Забезпечення консультаційних послуг та вказівок для організації з метою покращення якості та контролю інформаційних систем.
8. Визначення можливостей для процесних удосконалень IT -політик та практик.

Домен 2 - Загальне управління та менеджмент IT

1. Оцінювання стратегії IT для узгодження зі стратегіями та цілями організації.
2. Оцінювання ефективності структури управління IT та організаційної структури IT.

10/14 Radyshcheva Str., 03124, Kyiv, Ukraine
Tel.:+380 44 594 80 18; training@issp.com
www.issp.training

3. Оцінювання управління IT-політикою та практиками.
4. Оцінювання політики та практики IT організації на відповідність нормативним та правовим вимогам.
5. Оцінювання управління IT -ресурсами та портфоліо для узгодження зі стратегією та цілями організації.
6. Оцінювання політики та практики управління ризиками в організації.
7. Оцінювання управління IT та моніторинг контролів.
8. Оцінювання моніторингу та звітність за ключовими показниками ефективності IT (KPI).
9. Оцінювання відповідності вимогам бізнесу процесів відбору IT -постачальників та управління контрактами.
10. Оцінювання практики управління IT-сервісами відповідно бізнес-вимог.
11. Проведення періодичного огляду інформаційних систем та архітектури підприємства.
12. Оцінювання політики та практики управління даними.
13. Оцінювання програми інформаційної безпеки, з метою визначення її ефективності та відповідності стратегії і цілям організації.
14. Оцінювання потенційних можливостей та загроз, пов'язаних з новими технологіями, нормативними актами та галузевими практиками.

Домен 3 - Отримання, розробка та впровадження інформаційних систем

1. Оцінка відповідності бізнес-критеріїв та запропонованих змін у інформаційних системах з цілями бізнесу.
2. Оцінювання політики та практик управління проектами в організації.
3. Оцінювання контролів на всіх етапах життєвого циклу розробки інформаційних систем.
4. Оцінювання готовності інформаційних систем до впровадження та міграції у виробництво.
5. Проведення огляду систем після впровадження, з метою визначення відповідності результатів проекту, контролів та вимог.
6. Оцінювання політики та практик управління змінами, конфігурацією, релізами та патчами.

Домен 4 - Операції інформаційних систем та стійкість бізнесу

1. Оцінювання здатності організації продовжувати свою діяльність.
2. Оцінювання відповідності вимогам бізнесу практик управління IT-сервісами.
3. Проведення періодичного огляду інформаційних систем та архітектури підприємства.
4. Оцінювання IT-операцій з метою визначення ефективності їх контролю та їх можливість підтримувати цілі організації.
5. Оцінювання практик підтримки IT, з метою визначення ефективності їх контролю та їх можливість підтримувати цілі організації.
6. Оцінювання практики управління базами даних.
7. Оцінювання політики та практики управління даними.
8. Оцінювання політики та практики управління проблемами та інцидентами.
9. Оцінювання політики та практики управління змінами, конфігурацією, релізами та патчами.
10. Оцінювання обчислення кінцевого користувача, з метою визначення ефективності контролю процесів.

Домен 5 - Захист інформаційних активів

1. Проведення аудиту відповідно до стандартів аудиту ІБ та стратегії аудиту ІБ на основі ризиків.
2. Оцінювання політики та практики управління проблемами та інцидентами.

3. Оцінювання політики та практики інформаційної безпеки та конфіденційності в організації.
4. Оцінювання контролів доступу, з метою визначення відповідності заходів охорони інформаційних активів.
5. Оцінювання контролів логічної безпеки для перевірки конфіденційності, цілісності та доступності інформації.
6. Оцінювання практики класифікації даних для узгодження з політиками організації та зовнішніми вимогами.
7. Оцінювання політики та практики, пов'язаних з управлінням життєвим циклом активів.
8. Оцінювання програми інформаційної безпеки, з метою визначення її ефективності та відповідності стратегії і цілям організації.
9. Тестування технічної безпеки з метою виявлення потенційних загроз та вразливостей.
10. Оцінювання потенційних можливостей та загроз, що пов'язані з новими технологіями, нормативними актами та галузевими практиками.