CRISC – Certified in Risk and Information Systems Control

Про курс:

Дана сертифікація підтверджує досвід у визначенні та управлінні IT-ризиками підприємства, а також у впровадженні та підтримці засобів контролю інформаційних систем. CRISC призначений для IT та бізнес-фахівців середньої ланки, які виявляють і керують ризиками шляхом розробки, впровадження та підтримки відповідних контролів інформаційних систем (IC). Сертифікація CRISC підтверджує навички та знання щодо захисту сучасного підприємства від ескалації загроз.

Для кого:

- Директори / менеджери / консультанти з безпеки
- Директори та менеджери з питань відповідності /ризиків / конфіденційності
- Директори / менеджери / консультанти з аудиту IT
- Спеціалісти відділу комплаєнсу / ризиків / контролю

Курс допоможе зрозуміти основні концепції та вивчити такі сфери:

- Управління через політики
- Оцінка IT ризиків
- Реагування на ризики та звітування
- Інформаційні технології та безпека

Програма курсу:

Домен 1: Ідентифікація IT-ризиків

Визначати всесвіт IT-ризиків, для виконання стратегії управління IT-ризиками, підтримки бізнес-цілей і узгодження зі стратегією управління ризиками підприємства (ERM).

1. Збір та опрацювання інформації, включаючи наявну документацію, щодо внутрішнього і зовнішнього бізнес-середовища та IT-середовища організації, для визначення потенційного або здійсненого впливу IT-ризику на бізнес-цілі та діяльність організації
2. Визначення потенційних загроз та вразливостей для людей, процесів і технологій організації, для аналізу IT-ризиків.
3. Розробка комплексного набору сценаріїв IT-ризиків на основі наявної інформації, для визначення потенційного впливу на бізнес-цілі та діяльність бізнесу.
4. Визначення ключових зацікавлених сторін для сценаріїв IT-ризиків, для встановлення підзвітності.
5. Створення реєстру IT-ризиків, щоб забезпечувати, що визначені сценарії IT-ризиків враховуються та включаються в профіль ризиків для всього підприємства.

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

6. Визначення схильності і толерантності до ризику, встановлений вищим керівництвом і ключовими зацікавленими сторонами, для забезпечення відповідності бізнес-цілям.
7. Співпраця над розробкою програми поінформованості про ризики та проведення тренінгів, для розуміння ризиків зацікавленими сторонами та сприяння культурі усвідомлення ризиків.

Домен 2 - Оцінка IT-ризиків

Аналіз та оцінка IT-ризиків, для визначення ймовірності і впливу на бізнес-цілі, для забезпечення прийняття рішень на основі ризиків.

1. Аналізувати сценарії ризику на основі організаційних критеріїв (наприклад, організаційної структури, політик, стандартів, технологій, архітектури, засобів контролю), для визначення ймовірності впливу ідентифікованого ризику.
2. Визначати поточний стан існуючих засобів контролю та оцінювати їх ефективність для зменшення IT-ризиків.
3. Перегляд результатів аналізу ризиків і контролів, для оцінки розбіжностей між поточним і бажаним станом середовища IT-ризику.
4. Забезпечення наявності «власника» ризику, для встановлення чітких ліній відповідальності.
5. Повідомлення результатів оцінки ризику вищому керівництву та відповідним зацікавленим сторонам для прийняття рішень на основі оцінки ризику.
6. Актуалізація реєстру ризиків результатами оцінки ризиків.

Домен 3 - Реагування на ризики та їх зменшення

Визначати варіанти реагування на ризики та оцінка їх ефективності і результативності, для управління ризиками відповідно до бізнес-цілей.

1. Консультування з власниками ризиків, щоб вибрати рекомендовані заходи реагування на ризики, узгодити їх з бізнес-цілями та забезпечити прийняття обґрунтованих рішень щодо ризиків.
2. Консультування з власниками ризиків або допомога їм у розробці планів дій щодо ризиків, щоб переконатися, що плани включають ключові елементи (наприклад, відповідь, вартість, цільовий термін).
3. Консультування щодо розробки та впровадження або коригування засобів контролю, для забезпечення прийнятного рівня управління ризиком.
4. Забезпечення наявності «власника» контролів, для встановлення чітких ліній підзвітності.
5. Допомога власникам засобів контролю в розробці процедур контролю та документації для ефективного та ефективного здійснення контролю.
6. Оновлення реєстру ризиків для відображення змін у ризиках і реагуванні керівництва на ризики.
7. Забезпечення реагування на ризики, відповідно до планів дій щодо ризику.

Домен 4 - Моніторинг і звітність про ризики та контролі

Відстеження та звітування про IT-ризики та засоби контролю відповідним зацікавленим сторонам, для забезпечення ефективності і результативності стратегії управління IT-ризиками та її узгодження з бізнес-цілями.

1. Визначення і встановлення ключових показників ризику (KRI) і порогових значень на основі наявних даних, щоб уможливити моніторинг змін ризику.2.
2. Моніторинг і аналіз ключових показників ризику (KRI) для виявлення змін або тенденцій у профілі IT-ризику.
3. Звітування про зміни або тенденції, пов’язані з профілем IT-ризику, для допомоги керівництву та зацікавленим сторонам у прийнятті рішень.
4. Сприяння визначенню метрик і ключових показників ефективності (KPI), для вимірювання ефективності контролю.
5. Моніторинг і аналіз ключових показників ефективності (KPI) для виявлення змін або тенденцій, пов’язаних із середовищем контролю, і визначення ефективності та результативності засобів контролю.
6. Перегляд результатів контрольних оцінок для визначення ефективності контрольного середовища.
7. Звітування відповідним зацікавленим сторонам про ефективність, зміни або тенденції в загальному профілі ризику та середовищі контролю для прийняття рішень.