BDO ACADEMY

ПРОГРАМА
курсу сертифікації CISA від ISACA

Вступ

1.Загальна інформація про іспит
2. Процедура сертифікації

Розділ 1. Процес аудиту інформаційних систем

1.Планування
- 1.1 Стандарти аудиту ІС, настанови та кодекси етики
- 1.2 Бізнес-процеси
- 1.3 Типи контролів
- 1.4 Ризик-орієнтоване планування аудиту
- 1.5 Види аудитів і оцінок

2. Виконання
- 2.1 Управління проєктами аудиту
- 2.2 Методика вибірки
- 2.3 Методи збору аудиторських доказів
- 2.4 Аналіз даних
- 2.5 Методи звітування та комунікації
- 2.6 Забезпечення якості та вдосконалення процесу аудиту

Розділ 2. Корпоративне та операційне управління IT

1. Корпоративне управління IT
- 1.1. Управління IT та IT-стратегія
- 1.2 Пов'язані з IT фреймворки
- 1.3 IT-стандарти, політика та процедури
- 1.4 Організаційна структур а
- 1.5 Архітектура підприємства
- 1.6 Управління ризиками на підприємстві
- 1.7 Моделі зрілості
- 1.8 Закони, положення та галузеві стандарти, що впливають на організацію

2. Операційне управління IT
- 2.1 Управління IT-ресурсами
- 2.2 Залучення та управління постачальниками IT-послуг
- 2.3 Моніторинг і звітність роботи IT
- 2.4 Забезпечення якості та управління якістю IT

Розділ 3. Придбання, розробка та впровадження інформаційних систем

1. Придбання та розробка інформаційних систем
- 1.1 Стратегічне і операційне управління проєктами
- 1.2 Бізнес-аналіз та оцінка здійсненності
- 1.3 Методології розробки системи
- 1.4 Ідентифікація та дизайн контролю

Розділ 4. Процеси експлуатації, обслуговування та підтримки IT

1. Експлуатація інформаційних систем
- 1.1 Комп'ютерні апаратні компоненти та архітектури
- 1.2 Управління IT-активами
- 1.3 Системні інтерфейси

ISACA

1.4 Обчислення для кінцевих користувачів
1.5 Управління даними
1.6 Управління продуктивністю систем
2. Впровадження інформаційних системи
2.1 Методології тестування
2.2 Управління конфігурацією та випуском
2.3 Міграція систем, розгортання інфраструктури та перетворення даних
3. Огляд після впровадження
1.7 Управління проблемами та інцидентами
1.8 Управління змінами, конфігураціями, випуском і виправленнями
1.9 Управління рівнем IT-послуг
1.10 Управління базами даних
2. Стійкість бізнесу
2.1 Аналіз впливу на бізнес (BIA)
2.2 Стійкість систем
2.3 Резервне копіювання, зберігання і відновлення даних
2.4 План безперервності бізнесу (BCP)
2.5 Плани відновлення після стихійних лих (DRP)

Розділ 5. Захист інформаційних активів

1.Захист і контроль інформаційних активів
1.1 Вступ
1.2 Фреймворки, стандарти та рекомендації щодо захисту інформаційних активів
1.3 Принципи конфіденційності
1.4 Фізичний доступ і контролі навколишнього середовища
1.5 Управління ідентифікацією та доступом
1.6 Безпека мережі та кінцевих точок
1.7 Класифікація даних
1.8 Шифрування даних і методи, пов'язані з шифруванням
1.9 Інфраструктура відкритих ключів (PKI)
1.10 Інтернет-комунікаційні технології
1.11 Віртуалізовані середовища
1.12 Мобільні, бездротові та пристрої Інтернету речей (IOT)
2. Управління подіями безпеки
2.1 Навчання та програми з підвищення обізнаності щодо безпеки
2.2 Методи атаки на інформаційну систему
2.3 Інструменти та методи перевірки безпеки
2.4 Засоби та методи моніторингу безпеки
2.5 Управління реагуванням на інциденти
2.6 Збір доказів і криміналістика

Пробний іспит CISA ©

1. Структура іспиту
2. Детальний розбір відповідей на питання.