ПРЕДЛОЖЕНИЕ

На обучающий тренинг:

Курс EPC01: Подготовительный тренинг к экзаменам CISSP, CISM (Exam Prep Course)

- **Предварительный уровень подготовки**: понимание основ ИТ и ИБ.
- **Тренер:** Эксперт-практик CISSP, CISM, CISA
- **Статус:** Exam Prep Course
- **Длительность обучения** – 5 (пять) дней (45 ак.часов)
- **Форма обучения** – аудиторные занятия
- **Место проведения** – На базе центра повышения квалификации: «INTELLA»

г.Алматы, ул.Ауэзова, 60 БЦ “Almaty Residense” 6 этаж офис 17а тел. +7 (727) 355 02 34
г.Астана, 010000, г. Астана, р-н Есиль ул. Д. Кунаева, 29/1, оф.1903 тел. +7 (7172) 28 00 82

- **Даты проведения** - ведется набор
- **Расписание –** с 10.00 до 18.00, обед с 13.00 до 14.00.
- **В стоимость включено:** Раздаточный материал (в электронном и печатном виде) Кофе-брейки

Цель курса:

Данный курс готовит к получению сертификаций, являющихся Золотым Стандартом в сфере ИБ: Certified Information Systems Security Professional (CISSP) от консорциума ISC2 и Certified Information Security Manager от ассоциации ISACA. Всем четырем доменам экзамена CISM– Certified Information Security Manager, соответствуют модули курса, изучаемые в первые 3 дня тренинга.

Ориентирован на: Руководителей/экспертов в области обеспечения информационной безопасности, ИТ-аудиторов.

Преимущества сертификации CISSP:

- Получение актуальных знаний в области информационной безопасности;
- Подтверждение собственной квалификации;
- Защита активов организации на основании лучших международных практик по обеспечению ИБ;
- Приобщение к авторитетному обществу специалистов по информационной безопасности.

Результат обучения:

система знаний, необходимая для успешной сдачи экзамена **CISSP/CISM**

Контакты:

Исполнительный директор ТОО «INTELLA» Диана Фролова df@intella.kz +7 777 552 74 22

Асель Муханмеджанова asel@pacifica.kz (Астана) + 7 (7172) 28-00-82

Татьяна Бережная tb@intella.kz (Алматы) +7 (727) 355 02 34

Курс EPC01: Подготовительный тренинг к экзаменам CISSP, CISM (Exam Prep Course)

Модуль 0. Оценочный тест 250 вопросов (предварительный или во время 1-го занятия, в электронном или печатном виде).

1. Знакомство с экзаменом.
    - Все домены СВК.
2. Безопасность и управление рисками.
    - Понимание и применение концепций конфиденциальности, целостности и доступности.
    - Домашнее задание 1 в форме теста: 25 вопросов
3. Безопасность активов
    - Категорирование ресурсов. Определение и контроль владельцев. Защита персональных данных. Контроль сроков хранения. Определение механизмов контроля. Управление жизненным циклом ресурсов.
    - Домашнее задание 3 в форме теста. 25 вопросов
4. Субъекты и управление доступом
    - Физический и логический контроль доступа к активам. Управление идентификацией и аутентификацией субъектов. Субъект как услуга. Внедрение и управление механизмами авторизации. Атаки на механизмы контроля. Управление жизненным циклом субъекта и его полномочий.
    - Домашнее задание 4 в форме теста. 25 вопросов
5. Оценка и тестирование безопасности
    - Разработка и проверка стратегий оценки и тестирования. Тестирование механизмов контроля. Сбор информации о процессах ИБ. Анализ и отчетность. Внутренний и внешний аудит ИБ.
    - Домашнее задание 5 в форме теста. 25 вопросов
6. Безопасность операций
    - Понимание и поддержка процедур расследования инцидентов. Понимание требований законов и регуляторов в части проведения расследований. Организация журналирования и мониторинга. Безопасное использование ресурсов. Понимание и применение фундаментальных концепций безопасности операций. Реализация техник защиты ресурсов. Управление инцидентами. Превентивные меры. Управление уязвимостями и обновлениями. Понимание и участие в процессах управления внесением изменений. Внедрение стратегий восстановления. Внедрение процессов восстановления после катастроф. Тестирование планов восстановления после катастроф. Участие в планировании непрерывности бизнеса. Реализация и управление физической безопасностью. Участие в проверке лояльности персонала организации.
    - Домашнее задание 6 в форме теста. 25 вопросов
7. Проектирование систем защиты
    - Проектирование с учетов принципов ИБ. Понимание фундаментальных концепций моделей безопасности. Определение комплекса мер по защите соответствующего выбранной модели. Понимание возможностей механизмов защиты. Выявление и устранение уязвимостей в архитектуре системы защиты, ее реализации и компонентах. Уязвимости в веб-, мобильных и встроенных системах. Применение криптографии. Применение

принципов безопасности к контролируемой территории и зданию. Разработка и внедрение физических мер защиты.
    - Домашнее задание 7 в форме теста. 25 вопросов
8. Безопасность сетей и коммуникаций
    - Применение принципов ИБ к архитектуре сети. Компоненты безопасной сети. Организация безопасных каналов связи. Предотвращение и борьба с атаками на сеть.
    - Домашнее задание 8 в форме теста. 25 вопросов
9. Безопасная разработка ПО
    - Понимание и применение принципов ИБ на всех этапах жизненного цикла разработки ПО. Реализация механизмов контроля в среде разработки. Оценка эффективности контроля. Оценка рисков ИБ, порождаемых приобретенным ПО.
    - Домашнее задание 9 в форме теста. 25 вопросов
10. Итоговый тест 250 вопросов.

Дополнительная информация:

Соответствие доменов экзамена CISSP и модулей курса однозначное. Всем четырем доменам экзамена CISM соответствуют модули курса, изучаемые в первые 3 дня семинара (по модуль 6 включительно).

Методические материалы: Учебное пособие с теоретической и практической частью.
Документ об окончании курса: Свидетельство учебного центра. Дополнительно выдаются результаты итогового тестирования и рекомендательное письмо, заверенные инструктором с квалификацией CISSP, CISM,CISA

- Точное место и способ проведения тренинга уточняйте у менеджера по обучению
- При группах от 3 человек стоимость и место проведения тренинга по согласованию с Заказчиком
- Тренинги могут проводиться в г. Алматы, г. Астана, г. Москва или дистанционно