Контакти для зв'язку з приводу замовлення або запитань:
Телефон: +380966852884
Електронна пошта: sales@pakurity.com
Веб-сайт: https://pakurity.com/

Навчальний курс «IT аудит»

Версія: 2021-07-06
Автор: Гліб Пахаренко
Тривалість: 3 дня

Навчальний курс дозволяє учасникам отримати широкий набір знань для планування, проведення IT аудиту та управління його корпоративними програмами. Ви будете мати усі необхідні навички для вирішення найскладніших проблем, які включають:

- планування аудиту та складання звітності
- аудит безперервності бізнесу
- розробку програмного забезпечення та аудит життєвого циклу впровадження системи
- операційні системи, бази даних, аудит конфігурації мережевого обладнання.

Це виключно практичне навчання! Ви відразу будете працювати. Тренінг адаптований для аудиторії, яка представляє студентів із абсолютно різним досвідом. Якщо Ви - просто новачок, то будете вирішувати прості завдання. Якщо Ви - спеціаліст, у вас буде набір дуже складних завдань. Отриманий досвід обов'язково підвищить Вашу цінність для співробітників та клієнтів та принесе надзвичайний рівень професійної впевненості особисто Вам.

Навчальний курс призначений для:

- IT аудиторів
- Спеціалістів з IT безпеки
- Спеціалістів з якості IT
- IT менеджерів.

Програма навчального курсу «IT аудит»

Розділ 1. IT аудит

1. Принципи забезпечення IT (ITAF)
2. Статут/сфера повноважень аудиту
3. Незалежність аудитора
4. Професійний підхід
5. Твердження аудиту
6. Критерії аудиту
   - Програми аудиту ISACA
   - Інструкції IIA з аудиту
   - Принципи та критерії довірчих послуг
   - COBIT
   - COSO
   - ISO 27001
   - Інші джерела критеріїв
7. Планування аудиту. Підхід оснований на ризику
8. Продуктивність аудиту
9. Матеріальність знахідок аудиту
10. Докази аудиту
11. Методи збору доказів
12. Формування вибірки
13. Використання роботи інших експертів
14. Звітність
15. Обробка порушень законодавства
16. Дії після аудиту
17. Контрольне оточення
18. Дизайн контролів
19. Ефективність контролів
20. Моніторинг контролів

Наведена програма може бути змінена відповідно до потреб компанії/організації.

Контакти для зв'язку з приводу замовлення або запитань:
Телефон: +380966852884
Електронна пошта: sales@pakurity.com
Веб-сайт: https://pakurity.com/

21. Практичні групові завдання.

Розділ 2. Керівництво та управління діяльністю IT

1. Стратегія IT
2. Архітектура IT
3. Кількісні показники IT
4. Організація IT
5. Управління IT послугами
6. Каталог послуг
7. Управління інцидентами
8. Управління змінами
9. Управління релізами
10. Управління проблемами
11. Інвестиції IT
12. Ризики IT
13. End-user computing
14. Тіньові IT ресурси
15. Хмарні IT ресурси
16. Політика «Принеси свій пристрій» (Bring your own device, BYOD)
17. Аутсорсинг IT
18. Практичні групові завдання.

Розділ 3. Розробка та впровадження інформаційних систем

1. Життєвий цикл розробки та впровадження системи
2. Принципи контролю управління проєктами
3. Методології розробки систем
4. Бізнес-модель проєкту
5. Техніко-економічне обґрунтування
6. Специфікація вимог
7. Дизайн та архітектура
8. Процес закупівель
9. Кодування
10. Впровадження
11. Тестування
12. Передача в продуктивне (експлуатаційне) середовище
13. Оперативна підтримка
14. Зняття з експлуатації
15. Міграції
16. Закриття проєкту
17. Практичні групові завдання.

Розділ 4. IT операції

1. Управління запасами та активами
2. Управління патчами (внесенням виправлень)
3. Технічне обслуговування обладнання
4. Ліцензування
5. Планування потужності
6. Моніторинг роботи та доступності
7. Комунікації
8. Управління центром обробки даних
9. Фізична інфраструктура мережі
10. Практичні групові завдання.

Розділ 5. Безперервність діяльності і аварійне відновлення

1. Управління безперервністю діяльності
2. Ініціювання та управління проєктами безперервності діяльності
3. Оцінка впливу на діяльність

Наведена програма може бути змінена відповідно до потреб компанії/організації.

4. Цільова точка відновлення/Цільовий час відновлення (Recovery Point Objective, RTO/Recovery Time Objective, RPO)
5. Стратегії відновлення
6. Тестування плану безперервності діяльності
7. Фази аварії:
   - Підготовка
   - Первинна реакція
   - Виправлення
   - Відновлення
   - Діяльність після інциденту
8. Практичні групові завдання.

Розділ 6. Забезпечення інформаційної безпеки

1. Політики, стандарти та процедури інформаційної безпеки
2. Ролі інформаційної безпеки та організаційні структури
3. Безпека людських ресурсів
4. Класифікація та обробка даних
5. Ключові процеси
6. Управління ризиками інформаційної безпеки
7. Обробка випадків
8. Програми підвищення обізнаності
9. Управління ідентифікацією та доступом
10. Систем виявлення вторгнень/Система запобігання вторгнень (Intrusion detection system, IDS/Intrusion Prevention System, IPS)
11. Система запобігання втрати даних (Data Loss Prevention, DLP)
12. Система управління інформаційною безпекою та подіями інформаційної безпеки (Security information and event management, SIEM)
13. Інфраструктура відкритих ключів (Public key infrastructure, PKI)
14. 802.11x, захист доступу до мережі (Network Access Protection, NAP) та контроль доступу до мережі
15. Ризики віддаленого доступу та дистанційної роботи
16. Управління правами
17. Рішення проти шкідливих програм
18. Контроль фізичної безпеки
19. Контроль шахрайства
20. Практичні групові завдання.

Розділ 7: Аспекти аудиту

1. Аудит планування ресурсів підприємства (Enterprise Resource Planning, ERP)
2. Аудит управління відносинами з клієнтами (Customer Relationship Management, CRM)
3. IP-телефонія (Voice over IP, VOIP)
4. Віртуалізація
5. Практичні групові завдання.

Семінари:

- Аудит Windows
- Аудит Linux
- Аудит мережі, віртуальної приватної мережі (Virtual Private Network, VPN) та мережевого екрану
- Аудит інфраструктури відкритих ключів (PKI)
- Аудит бази даних (MySQL і Oracle)
- Аудит вед-додатку (PHP)
- Аудит мобільного додатку (Android).