

Практика ведения аудита IT. Оценка состояния информационной системы компании и ее соответствие потребностям бизнеса

За четыре дня в доступной форме опытные эксперты-практики донесут до участников практические рекомендации по ведению аудита IT. На курсе будут рассмотрены вопросы аудита компонентов управления IT-структуры, а также контрольных мер на этапе жизненного цикла информационных систем.

Дата проведения: 21 - 24 октября 2024 с 10:00 до 17:30

Артикул: MC24951

Вид обучения: Курс повышения квалификации

Формат обучения: Онлайн-трансляция

Срок обучения: 4 дня

Продолжительность обучения: 32 часа

Стоимость участия: 50 000 руб.

Для участников предусмотрено: Методический материал.

Документ по окончании обучения: По итогам обучения слушатели, успешно прошедшие итоговую аттестацию по программе обучения, получают Удостоверение о повышении квалификации в объеме 32 часов (в соответствии с лицензией на право ведения образовательной деятельности, выданной Департаментом образования и науки города Москвы).

Для кого предназначен

Внутренних и внешних аудиторов и контролёров, IT-специалистов.

Цель обучения

Получить актуальные знания в области ведения аудита IT.

Результат обучения

В-результате обучения участники: получают навык оценки состояния информационной системы компании и её-соответствие потребностям бизнеса.

Это мероприятие можно заказать в корпоративном формате (обучение сотрудников одной компании).

Программа обучения

День-1.

Стандарты, используемые в-ИТ-аудите:

- Соответствие политики, стандартов и-процедур лучшим практикам информационной безопасности.
- Разработка и-внедрение стратегии риск-ориентированной стратегии ИТ-аудита в-соответствие со-стандартами.
- Планирование ИТ-проверок с-целью обеспечения уверенности, что информационные системы контролируемы, безопасны и-предоставляют пользу предприятию.
- Проведение ИТ-проверок в-соответствие со-стандартами и-планами.
- Подготовка отчетов по-результатам проверки.
- Корректирующие действия по-результатам проверки.

Аудит управления ИТ-рисками:

- Риски, связанные с-доступом в-ИТ-системы.
- Специфика управления ИТ-рисками.

Аудит компонентов управления ИТ-структуры:

- Организационные структуры в-области ИТ.
- Методы руководства-ИТ с-целью достижения целей предприятия.
- ИТ-стратегии с-точки зрения достижения бизнес-целей предприятия.
- Соответствие ИТ-политики и-стандартов ИТ-стратегии и-нормативным требованиям.
- Общие контрольные меры в-области ИТ.
- Системы контроля качества в-области-ИТ на-соответствие ИТ-стратегии и-эффективности с-точки зрения затрат.
- Приоритеты инвестиций в-ИТ.
- Договоры по-услугам ИТ.
- Степени информированности и-мониторинга-ИТ со-стороны высшего руководства.
- Процессы в-области обеспечения непрерывности бизнеса.

День-2.

Аудит приобретения, разработки, внедрение и-изменения информационных систем:

- Технично-экономических обоснований ИТ- проектов.
- Процесс разработки систем и-внесения изменений.
- Риски, возникающие при разработке и-внесении изменений.
- Практика управления ИТ-проектами на-предмет соблюдения бизнес-требований.
- Выполнение ИТ-проектов с-соблюдением сроков и-планов.
- Контрольные процедуры и-их-тестирование в-процессе разработки и-изменения программ.
- Контрольные меры на-этапе жизненного цикла информационных систем.
- Результаты проектов по-внедрения изменения информационных систем.

День-3.

Аудит эксплуатации, сопровождения и-поддержки информационных систем:

- Проведение периодических проверок-ИС на-предмет выполнения требований к-ним.
- Соглашения об-уровне ИТ-сервисов.
- Меры контроля на-стороне поставщиков ИТ-сервисов.
- ИТ-операции и-процедуры.
- Процессы сопровождения и-поддержки ИТ-инфраструктуры и-сервисов.
- Качество администрирования баз данных.
- Уровни загрузки мощностей ИТ-инфраструктуры.
- Практики управления инцидентами ИТ.
- Процедуры внесения изменений в-ИС и-резервирования данных.
- Планы восстановления после прерываний.

День-4.

Аудит безопасности и-контроля доступа:

- Дизайн, внедрения и-мониторинга мер контроля безопасности.
- Место ИТ-контроля в-контрольной среде компании.
- Типы контрольных процедур в-ИТ.
- Процесс классификации информации на-соблюдение корпоративных и-нормативных требований.
- Меры контроля физического доступа и-меры по-защите информационных активов от-воздействия окружающей среды.

- Процессы и-процедуры по-хранению, транспортировке и-уничтожению носителей информации с-точки зрения обеспечения безопасности.
- Контрольные процедуры и-их-тестирование.

Преподаватели

ПРЕПОДАВАТЕЛЬ

Эксперты - практики.