8 (495) 698-63-64
8 (800) 234-55-22
seminar@finkont.ru
www.finkont.ru

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

За три 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: 25 - 27 августа 2025 с 10:00 до 17:30

Артикул: СП13311

Вид обучения: Курс повышения квалификации

Формат обучения: Дневной

Срок обучения: 3 дня

Продолжительность обучения: 24часа

Место проведения: г. Санкт-Петербург, Лиговский проспект, 266с1, Бизнес Центр Премьер Лига (3 очередь), 4 этаж, из лифта направо. Станции метро «Московские ворота», «Технологический институт», «Обводный канал».

Стоимость участия: 50 000 руб.

Для участников предусмотрено: Методический материал, кофе-паузы.

Документ по окончании обучения: По итогам обучения слушатели, успешно прошедшие итоговую аттестацию по программе обучения, получают Удостоверение о повышении квалификации в объеме 24 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.

Результат обучения

В результате обучения участники получат: 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 IT-аудите:

- Соответствие политики, стандартов и процедур лучшим практикам информационной безопасности.

- Разработка и внедрение стратегии риск-ориентированной стратегии IT-аудита в соответствие со стандартами.
- Планирование IT проверок с целью обеспечения уверенности, что информационные системы контролируемы, безопасны и предоставляют пользу предприятию.
- Проведение IT проверок в соответствие со стандартами и планами.
- Подготовка отчетов по результатам проверки.
- Корректирующие действия по результатам проверки.

Аудит управления IT-рисками:

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

Аудит компонентов управления IT-структуры:

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

День 2.

Аудит приобретения, разработки, внедрение и изменения информационных систем:

- Технико-экономических обоснований IT- проектов.
- Процесс разработки систем и внесения изменений.
- Риски, возникающие при разработке и внесении изменений.
- Практика управления IT-проектами на предмет соблюдения бизнес-требований.
- Выполнение IT-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.

Аудит эксплуатации, сопровождения и поддержки информационных систем:

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

День 3.

Аудит безопасности и контроля доступа:

- Дизайн, внедрения и мониторинга мер контроля безопасности.
- Место IT-контроля в контрольной среде компании.
- Типы контрольных процедур в IT.
- 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.