INTERNATIONAL BUSINESS ACADEMY

+7 727 328 02 02/03 hotline 24/7

+7 702 777 44 11

Разработка и внедрение Системы менеджмента информационной безопасности в соответствии с требованиями международного стандарта ISO 27001:2022

Программа

Введение

Знакомство/ введение/ обзор курса/ представление слушателей

История стандартизации. Введение в ISO

Семь принципов менеджмента

Контекст компании

Понимание организации и её контекста применительно к рискам и структуре компании

Метод «5К», Методика «5 сил Майкла Портера», SWOT-анализ, PEST-анализ

- Кейс: взаимосвязь контекста, Политики и Целей

Заинтересованные стороны, требования и ожидания заинтересованных сторон

Понимание заинтересованных сторон. Связь заинтересованных сторон и контекста

- Практическая групповая работа: определение заинтересованных сторон

Принятые обязательства, взаимосвязь с контекстом компании

Оценка степени соответствия принятым обязательствам

Примеры методик оценки соответствия принятым обязательствам

- Практическая групповая работа: определение принятых обязательств

Область применения Системы менеджмента информационной безопасности (СМИБ)

Области применения СМИБ и связь её с контекстом

Бизнес-процессы

Процессный подход

Взаимосвязь контекста и процессов

Порядок идентификации процессов — лучшие практики

- Практическая групповая работа: идентификация процессов компании, построение Модели СМИБ

Варианты описания процессов

- Практическая групповая работа: описание ключевых бизнес-процессов компании

Критерии процессов (KPI)

Виды критериев: input KPI и output KPI

Взаимосвязь критериев и стратегии компании

- Практическая групповая работа: определение критериев процесса (input KPI и output KPI)
- Непрерывная оценка: тест по 4-му разделу ISO

Введение в риск-менеджмент

Распространённые мифы в области риск-менеджмента и их разоблачение

Система-1, Система-2 и понятие «ментальных ловушек»

- Интерактивная игра по ментальным ловушкам
- Групповая игра: принятие решений с учётом рисков — «парадокс Монти Холла»

Идентификация рисков

Ментальные ловушки на этапе идентификации рисков

- Интерактивная игра по ментальным ловушкам на этапе идентификации рисков

Методы идентификации рисков (из ISO 31010:2019):

— Декомпозиция цели и метод MECE (Mutually Exclusive & Collectively Exhaustive)

— «Мозговой штурм»

— База данных реализовавшихся рисков

— Метод «RIR — Risk Identification Report»

— Контрольные «чек-листы»

— Анализ влияния на деятельность («процессный подход»)

- Практическая групповая работа: идентификация рисков процесса с использованием метода MECE и готового промта для Искусственного интеллекта

Анализ риска

Ментальные ловушки на этапе анализа рисков

- Интерактивная игра по ментальным ловушкам на этапе анализа рисков

Методы анализ риска (из ISO 31010:2019):

— Метод «5 почему»

— Метод «галстук-бабочка»

— Метод «деревья решений»

— Метод имитационного моделирования «Монте-Карло» и др.

Примеры анализа рисков и заполнения Регистра рисков

- Практическая групповая работа: анализ риска с использованием метода «галстук-бабочка» (определение причин, последствий, текущих контрольных мероприятий и оценка их результативности и эффективности)

Определение степени риска

Ментальные ловушки на этапе оценивания рисков

- Интерактивная игра по ментальным ловушкам на этапе оценивания рисков

Различные варианты оценивания риска (качественный, количественный
и их комбинация из ISO 31010:2019)

Оценка и анализ влияния рисков на принимаемое решение

Способы визуализации итогов оценки: Карты рисков, Деревья решений, Скоринговая модель

- Кейс: скоринговая модель как инструмент приоритизации рисков СМИБ

Воздействие на риск

Ментальные ловушки на этапе воздействия на риск

- Интерактивная игра по ментальным ловушкам на этапе воздействия на риск

Шесть способов обработки риска

Выбор метода обработки риска

Примеры обработки риска

- Интерактивная игра по способам обработки рисков
- Кейс: определение мероприятий по минимизации рисков, метод «галстук-бабочка»

Мониторинг и анализ рисков

Ключевые рисковые показатели (КРП). Взаимосвязь КРП и KPI

- Кейс: КРП и KPI

Лидерство

Риск-ориентированное принятие решений

Методы повышения качества принимаемых корпоративных решений из методики «Decision Quality»

Взаимосвязь стратегии, контекста и Политики в области СМИБ

Рекомендации по разработке Политики в области СМИБ

- Практическая групповая работа: разработка / анализ существующей Политики в области СМИБ

Ответственность и полномочия

Методы описания действий по процессам (в виде регламентов/ контрольных

процедур)

Дизайн бизнес-процессов и контролей

Основные требования/ рекомендации по разработке контрольных процедур и частые ошибки

Цели СМИБ

Требования стандартов к целеполаганию

Взаимосвязь стратегии, контекста, Политики и Целей СМИБ

Лучшие практики по целеполаганию с учётом рисков

- Практическая групповая работа: разработка целей в области СМИБ
- Непрерывная оценка: тест по 5 и 6-му разделу ISO

Ресурсы

Определение необходимой компетентности персонала для функционирования процессов

Определение необходимой инфраструктуры для функционирования процессов

Внутрифирменная база знаний.

Эффективные коммуникации. Документированная информация.

- Непрерывная оценка. Тест по 7 разделу стандарта ISO.

Осуществление деятельности

Оценка рисков информационной безопасности

Обработка рисков информационной безопасности

- Сквозной Кейс: идентификация, оценка и обработка рисков информационной безопасности.
- Непрерывная оценка. Тест по 8 разделу стандарта ISO.

Проверка

Внутренний аудит СМИБ.

Порядок планирования, проведения и анализа результатов риск-ориентированного внутреннего аудита СМИБ.

Анализ СМИБ. Лучшие практики.

- Непрерывная оценка: тест по 9-му разделу ISO.

Улучшения

Корректирующие действия. Примеры и лучшие практики.

Постоянное улучшение.

- Непрерывная оценка: тест по 10-му разделу ISO.

Групповая игра «интерактивный разбор требований и ситуаций из ISO 27001»

INTERNATIONAL BUSINESS ACADEMY

+7 727 328 02 02/03 hotline 24/7

+7 702 777 44 11

РК, г. Алматы ул. Шашкина 24БЦ K Plaza офис 1 (уг. проспекта Аль-Фараби)

www.iba.kz

info@iba.kz