Практика организации и проведения аудита информационной безопасности в компании

Борисов Сергей Александрович

ЭЛВИС-ПЛЮС

Национальные стандарты по аудиту

- ГОСТ Р ИСО 19011-2012 Руководящие указания по аудиту систем менеджмента
- ГОСТ Р ИСО/МЭК 17021-2008 Требования к органам, проводящим аудит и сертификацию систем менеджмента
- ГОСТ Р ИСО/МЭК 27006—2008 Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности

ЭЛВИС-ПЛЮС

Стандарт Банка России в области аудита ИБ

- Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности» СТО БР ИББС-1.1-2007

ЭЛВИС-ПЛЮС

Термины и определения

- **Аудит -** систематический, независимый и документируемый процесс получения свидетельств аудита и объективного их оценивания с целью установления степени выполнения согласованных критериев аудита
- **Критерии аудита -** совокупность политик, процедур или требований, используемых в качестве эталона, в соотношении с которым сопоставляют свидетельства аудита, полученные при проведении аудита
- **Свидетельство аудита -** записи, изложение фактов или другая информация, которые связаны с критериями аудита и могут быть проверены

ЭЛВИС-ПЛЮС

Термины и определения

- **Выводы (наблюдения) аудита -** результаты оценки собранных свидетельств аудита на соответствие критериям аудита
- **Заключение по результатам аудита -** выходные данные аудита после рассмотрения целей аудита и всех выводов аудита
- **Заказчик аудита -** организация или лицо, заказавшие аудит
- **Проверяемая организация**: Организация, подвергающаяся аудиту
- **Аудитор -** лицо, которое проводит аудит
- **Группа по аудиту -** один или несколько аудиторов, проводящих аудит, при необходимости поддерживаемые техническими экспертами

ЭЛВИС-ПЛЮС

Термины и определения

- **Технический эксперт -** лицо, обладающее специальными знаниями или опытом, необходимыми группе по аудиту
- **Наблюдатель** - лицо, сопровождающее **группу по аудиту**, но не проводящее аудит
- **Сопровождающий -** лицо, назначаемое Компанией для оказания помощи и содействия группе по аудиту
- **Программа аудита** - совокупность мероприятий по проведению одного или нескольких аудитов, запланированных на конкретный период времени и направленных на достижение конкретной цели
- **Область аудита** - содержание и границы аудита

ЭЛВИС-ПЛЮС

Термины и определения

- **План аудита -** описание деятельности и мероприятий по проведению аудита
- **Риск** - воздействие неопределенности на достижение целей
- **Компетентность** - способность применять знания и навыки для достижения намеченных результатов
- **Соответствие** - выполнение требования
- **Несоответствие -** невыполнение требования
- **Система менеджмента -** система для разработки политики и целей и достижения этих целей

ЭЛВИС-ПЛЮС

Принципы проведения аудита

- **Целостность** — основа профессионализма
- **Беспристрастность** — обязательство предоставлять правдивые и точные отчеты
- **Профессиональная осмотрительность** — прилежание и умение принимать правильные решения при проведении аудита
- **Конфиденциальность** — сохранность информации
- **Независимость** — основа беспристрастности и объективности заключений по результатам аудита
- **Подход, основанный на свидетельстве**, — разумная основа для достижения надежных и воспроизводимых заключений аудита в процессе систематического аудита

ЭЛВИС-ПЛЮС

Управление программой аудита

- цели для программы аудита и отдельных аудитов;
- объем/количество/типы/места проведения и график проведения аудитов;
- процедуры программы аудита;
- критерии аудита;
- методы аудита;
- формирование группы (групп) по аудиту;
- необходимые ресурсы, включая расходы на командировки и размещение аудиторов;
- процессы, связанные с соблюдением конфиденциальности, обеспечением защиты информации и другие подобные вопросы.

Проведение аудита

Организация проведения аудита

- Установление первоначального контакта с Компанией
- Определение возможности проведения аудита

ЭЛВИС-ПЛЮС

Проведение аудита

Подготовка к проведению аудита на месте

- Выполнение анализа документов при подготовке к аудиту
- Подготовка плана аудита
- Распределение работ между членами группы по аудиту
- Подготовка рабочих документов

ЭЛВИС-ПЛЮС

Проведение аудита

Проведение аудита на месте

- Проведение предварительного совещания
- Выполнение анализа документов во время проведения аудита
- Обмен информацией во время проведения аудита
- Роль и обязанности сопровождающих лиц и наблюдателей
- Сбор и верификация информации
- Формирование выводов аудита
- Подготовка заключений по результатам аудита
- Проведение заключительного совещания

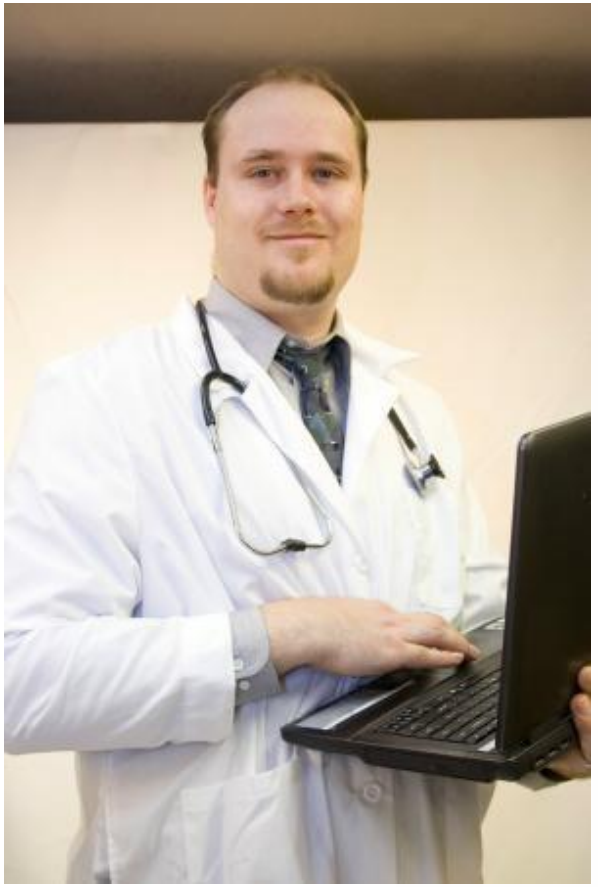
Проведение аудита

Подготовка и рассылка отчета по аудиту

- Подготовка отчета по аудиту
- Рассылка отчета по аудиту

Проведение аудита

- Завершение аудита
- Действия по результатам аудита



Ваши вопросы?

Борисов Сергей Александрович