Аудит в сфере ИТ

19-20 апреля,
Виртуальный
тренинг

Комитас Степанян,
PhD, CRISC, CRMA, CobitF

Аудит в сфере ИТ

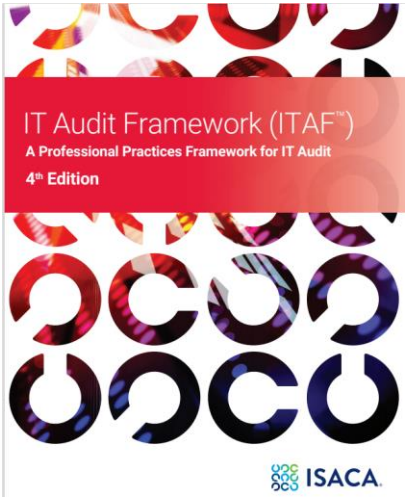
Программа

- ✓ Внутренний аудит и аудит в сфере ИТ
- ✓ Стандарты, механизмы и передовые практики аудита в сфере ИТ
- ✓ Обязанности, задачи и навыки, необходимые для проведения аудита в сфере ИТ
- ✓ Примеры

Что у нас есть

The Institute of Internal Auditors

ISACA



Аудит в области ИТ и заявления о стандартах обеспечения уверенности

Общие стандарты

1001 Устав аудита

1001.1 Функциональные подразделения аудита и обеспечения уверенности в области ИТ должны надлежащим образом задокументировать эту аудиторскую функцию в уставе аудита, указав **цель, обязанности, полномочия и порядок подотчетности.**

1004 Достаточные основания

1004.1 Специалисты-практики в области ИТ-аудита и обеспечения уверенности должны иметь достаточные основания полагать, что задание может быть выполнено в соответствии с применимыми стандартами аудита и обеспечения уверенности в области ИТ, а также, при необходимости, в соответствии с другими отраслевыми стандартами или применимыми нормативно-правовыми актами, в результате чего будет вынесено профессиональное заключение или сделаны соответствующие выводы.

ИТ-аудит и заявления о стандартах обеспечения уверенности

Общие стандарты

1006 Квалификация

1006.1 Специалисты-практики в области ИТ-аудита и обеспечения уверенности совместно с другими лицами, оказывающими помощь в проведении аудита и выполнении аудиторских заданий, должны обладать профессиональной компетенцией для выполнения требуемой работы.

1006.2 Специалисты-практики в области ИТ-аудита и обеспечения уверенности должны обладать знаниями в этой сфере, достаточными для выполнения их функций в области ИТ-аудита и обеспечения уверенности.

1008 Критерии

1008.1 Специалисты-практики в области ИТ-аудита и обеспечения уверенности должны выбрать такие критерии для оценки данного направления, которые являются объективными, полными, актуальными, надежными, измеримыми, понятными, широко признанными, авторитетными и понятными всем читателям и пользователям отчета.

Что у нас есть

3 Модель взаимодействий

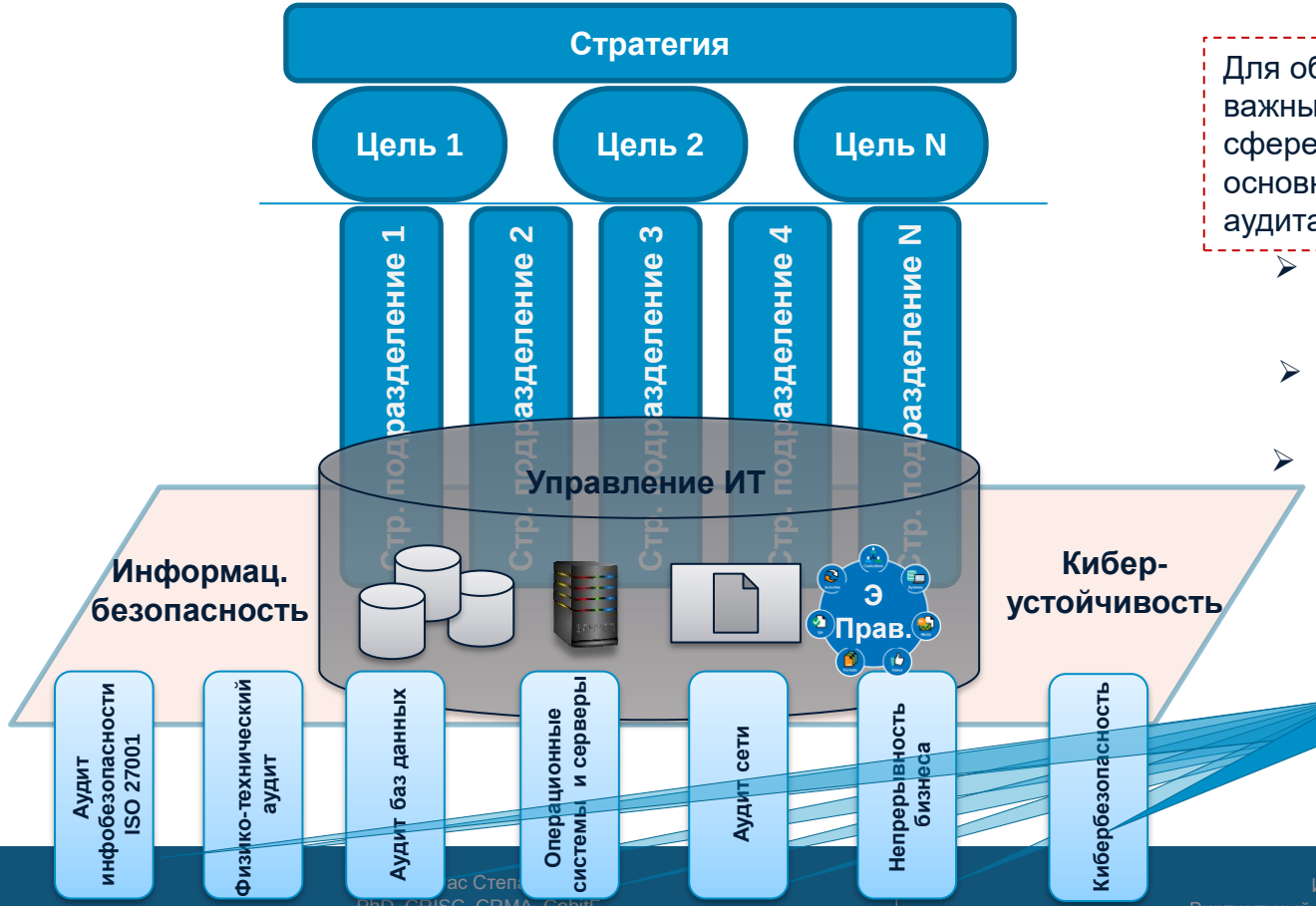
Подотчетность, отчетность

Делегирование, управление, ресурсы, надзор

Согласование действий, координация связей, сотрудничество

Подход и вселенная аудита в сфере ИТ

Подход и вселенная аудита в области ИТ



Для обеспечения охвата современных важных и стратегических рисков в сфере ИТ, ВА должен включить эти 3 основных процесса во вселенную ИТ-аудита.

- **Стратегическое и оперативное управление ИТ**
- **Информационная безопасность**
- **Кибер-устойчивость**

Навыки, необходимые для проведения аудита в сфере ИТ

Аудит общих средств контроля ИТ

Общие средства контроля ИТ, применяемые ко всей деятельности службы ИТ

- ✓ Управление доступом
- ✓ Управление изменениями
- ✓ Управление резервным копированием
- ✓ Управление инцидентами

Все внутренние аудиторы

Более углубленный ИТ-аудит

- ✓ Сетевой аудит
- ✓ Аудит СУБД
- ✓ Аудит активного каталога
- ✓ Аудит виртуализации
- ✓ Аудит кибербезопасности

ИТ-аудиторы

Пример: шесть основных средств контроля, наиболее часто проверяемые в ходе аудита общих средств контроля ИТ

Средство контроля 1: Физическая безопасность и защита сетевой информации от утечки

- ✓ Серверное помещение защищено системой доступа с помощью карты.
- ✓ Карты доступа в серверное помещение имеет ограниченное число сотрудников.
- ✓ В ЦОД установлены фальшполы, под которыми находятся детекторы воды.
- ✓ Сигнализация системы отопления, вентиляции и кондиционирования воздуха (HVAC) посылает электронные сообщения и запускает звуковые сигналы в случае сбоев в системах.
- ✓ Огнетушители серверного помещения проверяются ежеквартально.

Пример: шесть основных средств контроля, наиболее часто проверяемые в ходе аудита общих средств контроля ИТ

Средство контроля 2: Логическая безопасность

- ✓ Новым сотрудникам предоставляется доступ к системным ресурсам по согласованию с кадровой службой.
- ✓ Учетные данные уволенных сотрудников удаляются из системы в течение 15 минут с момента получения уведомления от кадровой службы.
- ✓ Для аутентификации пользователей, запрашивающих системные ресурсы, используется активный каталог Windows.

Пример: шесть основных средств контроля, наиболее часто проверяемые в ходе аудита общих средств контроля ИТ

Средство контроля 3: Управление изменениями

- ✓ Среда тестирования отделена от рабочей среды.
- ✓ Производственные и программные изменения перед вводом в эксплуатацию проверяются, документируются и утверждаются.

Пример: шесть основных средств контроля, наиболее часто проверяемые в ходе аудита общих средств контроля ИТ

Средство контроля 4: Резервное копирование и восстановление

- ✓ Резервное копирование данных производится ежедневно в соответствии с документально оформленным процессом и графиком.
- ✓ Для критически важных систем разработаны и ежегодно тестируются планы аварийного восстановления.

Пример: шесть основных средств контроля, наиболее часто проверяемые в ходе аудита общих средств контроля ИТ

Средство контроля 5: управление инцидентами

- ✓ Отчеты о работе формируются ежедневно и анализируются руководством ИТ-службы.
- ✓ Существует документально оформленная технология реагирования на инциденты, которая регулярно используется при реагировании на аномальные ситуации.

Пример: шесть основных средств контроля, наиболее часто проверяемые в ходе аудита общих средств контроля ИТ

Средство контроля 6: информационная безопасность

- ✓ Для защиты периметра сети от подозрительной деятельности используются межсетевые экраны.
- ✓ Для предотвращения ущерба от вирусов используется антивирусное программное обеспечение.
- ✓ Входящий и исходящий трафик данных контролируется непрерывно в режиме 24/7 для выявления потенциальных фишинговых атак, DDOS-атак и других попыток проникновения за периметр сети.
- ✓ Для проверки на наличие уязвимостей дважды в год проводится тестирование на проникновение.

Проведение аудита общих средств контроля ИТ

При проведении аудита общих средств контроля ИТ проверяется каждое средство контроля посредством комбинации методов:

1. Собеседования с ответственными сотрудниками (и их руководителями)
2. Изучение документации (в частности, письменных процедур, политик и технических руководств).
3. Наблюдения за работниками (например, наблюдение за тем, как человек выполняет задачи, связанные с использованием того или иного средства контроля)


How?
Where?
When?
Why?
Which?
What?
Who?
Why?