Министерство финансов
Республики Северная Македония

Департамент внутреннего аудита Министерства финансов: опыт проведения аудита общих средств контроля в сфере информационных технологий

Наташа Радеска Крстевска, CIA

Скопье, 2021 г.

Аудит общих средств контроля в сфере информационных технологий: основания

Определение внутреннего аудита

Внутренний аудит - это **деятельность по обеспечению независимой и объективной уверенности и консультаций, призванной повышать пользу для организации и совершенствовать её работу.** Внутренний аудит помогает организации достичь поставленных целей благодаря применению систематизированного и последовательного подхода к оценке и повышению **эффективности процессов управления рисками, контроля и корпоративного управления**.

Два основных принципа

- Способствовать развитию организации.
- Внимательно анализировать, применять упреждающий подход и ориентироваться на будущее.

В то время, когда:

- автоматизация процессов и использование информационных технологий (ИТ) – это наше настоящее и будущее, а
- пандемия COVID-19 усиливает эти тенденции.

Цели аудиторского задания по внутреннему аудиту, цели обеспечения увереннгости в ИТ-сфере и цели информационной безопасности

Главная цель аудита общих средств контроля в ИТ-сфере - **оценить проектирование, создание и функционирование системы внутренних общих средств контроля в сфере информационных технологий и содействовать ее непрерывному совершенствованию.**

Пять категорий целей обеспечения уверенности в ИТ-сфере:

1) **Доступность**
2) **Возможности**
3) **Функциональность**
4) **Подотчетность**
5) **Защищенность**

Три цели информационной безопасности:

1) **Доступность**
2) **Конфиденциальность**
3) **Целостность** (в том числе, **точность, полнота и безопасность**)

Риски, связанные с целями обеспечения уверенности в ИТ-сфере и целями информационной безопасности

Риск – это вероятность наступления события, оказывающего негативное влияние на достижение организацией ее целей.

При выявлении и оценке рисков внутренние аудиторы учитывают следующее:

- текущая оценка рисков руководством (например, на основе реестра рисков);
- оценка рисков, сформированная для годового плана;
- оценка рисков на основе результатов предыдущего аудита;
- предыдущие аудиторские отчеты.
- Иногда они также проводят «мозговые штурмы», чтобы выявить ключевые риски и средства контроля; в их ходе рассматривают следующие вопросы:
  - Что помешает деятельности в ИТ-сфере достичь своих целей применительно к области бизнеса и безопасности?
  - Как на такой вид деятельности повлияет отсутствие контроля?

Риски, связанные с целями обеспечения уверенности в ИТ-сфере и целями информационной безопасности

Реестр ИТ-ресурсов по группам связанных между собой категорий ресурсов:	Угроза	Уязвимость	Риск
Программное обеспечение (операционные системы, приложения, утилиты)	несанкционированное использование программного обеспечения	доступ к программному обеспечению	нарушение целостности и безопасности данных
	ненадлежащее использование программного обеспечения	сложность программного обеспечения	снижение качества данных и отчетов
	изменения в программном обеспечении	сложность программного обеспечения	неэффективное функционирование, нарушение целостности данных, недоступность
	вредоносное ПО (вирусы, спам, ...)	подверженность программного обеспечения воздействию вирусов	снижение качества услуг из-за частичной или полной потери программ и данных
	уничтожение файла программного обеспечения	особенности программного обеспечения и информации в электронной форме	невозможность возобновить эффективную работу в случае потери данных и программ
	стихийные бедствия	подверженность разрушению	прекращение функционирования в связи с частичным или полным уничтожением программного обеспечения и баз данных
	использование нелицензионного программного обеспечения	авторские права на программные продукты	несоблюдение юридических обязательств и отсутствие профессиональной поддержки и обслуживания
	некачественная и устаревшая документация	сложность программного обеспечения	низкое качество функционирования
	программные ошибки	характеристики программного обеспечения	снижение качества данных и отчетов
Аппаратные средства (компьютерное оборудование, такое как персональный компьютер, сервер, ноутбук, периферийные устройства и т. д.)	потеря или разрушение магнитных носителей	возможность переноса и подверженность уничтожению	потеря данных
	ненадлежащее администрирование систем	сложность системы	снижение функциональности и безопасности ИТ
	неисправность оборудования (компьютеры и сетевые устройства)	характеристики оборудования	снижение качества и эффективности
	ненадлежащее техническое обслуживание	подверженность повреждению	прерванные бизнес-процессы
	снижение безопасности использования	конфиденциальность систем и информации	снижение функциональности и безопасности ИТ
	неправильная конфигурация оборудования	сложность оборудования	ненадлежащая производительность компьютерной системы и сети
	отсутствие технической информации об оборудовании	сложность оборудования	ненадежная работа ИТ-оборудования
Инфраструктура (здания, офисы, кондиционирование, отопление ...)	несанкционированный доступ	доступность	снижение надежности информационных ресурсов
	затопление	неподходящее и незащищенное место хранения документации	частичное или полное уничтожение документации и оборудования
	землетрясение	несоблюдение правил сейсмостойкого строительства	частичное или полное уничтожение документации и оборудования

Административные средства контроля безопасности

Административные средства контроля безопасности включают в себя:

- **Политики** (порядок решения проблем и использование ИТ-инфраструктуры для решения проблем).
- **Стандарты** (помогают применять политики на практике, описывая действия, необходимые для соответствия положениям политики).
- **Процедуры** и **рекомендации** (показывают, как соблюдать политики, предоставляя подробные инструкции).

➢**Они очень важны для аудитора:**

- **Как критерии для оценки проектирования, внедрения и функционирования системы внутреннего контроля**.

Средства контроля информационных и связанных с ними технологий

Средства контроля информационных и связанных с ними технологий делятся на две широкие категории:

1) Общие средства контроля в ИТ-сфере – комплексный контроль на организационном уровне, охватывающий все компоненты систем, процессы и данные в ИТ-среде организации.

2) Средства контроля приложений – конкретные элементы управления, относящиеся к отдельным бизнес-процессам или приложениям.

Наиболее распространенные общие средства контроля в ИТ-сфере:

- **Физические средства контроля безопасности центра обработки данных.**
- **Логические средства контроля доступа к инфраструктуре, приложениям и данным.**
- **Средства контроля жизненного цикла разработки систем.**
- **Средства контроля процесса управления изменениями в программах.**
- **Средства контроля процесса управления резервным копированием и восстановлением систем и данных.**

Физическая безопасность – средства контроля физического доступа и параметров окружающей среды

Средства контроля физического доступа ограничивают круг лиц, которые могут физически получить доступ к системам (предотвращают несанкционированный доступ к компьютерным ресурсам):

- Доступ через дверь с клавишной кодонаборной панелью.
- Считыватели карт.
- Биометрические технологии.

Наиболее важные **средства контроля физического доступа и параметров окружающей среды**:

- Контроль температуры и влажности.
- Система пожаротушения (с применением газов вместо воды).
- Центр обработки данных не должен располагаться в помещениях, примыкающих к наружным стенам здания.
- Здание центра обработки данных не должно быть расположено в месте с высокой вероятностью подтопления.

Логические средства контроля безопасности

Логические средства контроля безопасности, которые предотвращают ненадлежащее использование или манипулирование файлами данных и программами и гарантируют, что получить доступ к компьютерным системам могут только правомочные лица, которые не имеют злого умысла:

- **Программное обеспечение для контроля доступа** (например, брандмауэр).
- **Пароли.**
- **Атрибуты файла** (например, только чтение, чтение/запись, архив, скрытый).
- **Матрицы контроля доступа** (таблицы или списки авторизованных пользователей или устройств).
- **Автоматический выход из системы (отключение)** для неактивного информационного терминала.
- **Журнал доступа к системе.**
- **Шифрование.**
- **Контролируемое уничтожение документов.**
- **Специалист по безопасности** (например, директор по информационной безопасности).

Средства контроля жизненного цикла разработки систем

Подход на основе жизненного цикла разработки систем (Systems Development Life-Cycle, SDLC) – традиционная методология, применяемая для разработки крупных, высокоструктурированных прикладных систем**,** основным преимуществом которой является **повышенная управляемость и контролируемость процесса разработки.** Методология предусматривает следующие пять шагов:

- Инициирование, проверка осуществимости и планирование.
- Анализ и определение требований.
- Проектирование систем.
- Приемка, установка и внедрение.
- Эксплуатация и техническое обслуживание.

Приложения, разработанные конечными пользователями, для которых не применялся описанный выше подход, могут не подвергаться независимому внешнему анализу системными аналитиками и могут не соответствовать применимым стандартам, средствам контроля, процедурам обеспечения качества и документации; кроме того, их интеграция с другими информационными системами может быть затруднена (что делает их применение более рискованным).

Средства контроля процесса управления изменениями в программах

Управление изменениями основано на процессах, которые управляют изменениями в производственных системах (например, улучшениями, обновлениями, инкрементными исправлениями и пакетами исправлений). Основной целью является поддержание и улучшение бизнес-процессов организации с минимальным воздействием и риском для производственных систем; для этого способ управления изменениями должен быть определенным, повторяемым и предсказуемым.

- Основные факторы риска **неэффективного управления изменениями**:

1) Несанкционированные изменения.

2) Незапланированные отключения.

3) Низкий процент успешных изменений.

4) Большое количество экстренных изменений.

5) Задержки при реализации проектов.

Средства контроля:

Средства упреждающего контроля:

- разделение обязанностей;
- рассмотрение и одобрение изменений;
- ограничение круга лиц, которые могут повышать уровень доступа к производственным данным и программам.

Средства обнаружения:

- мониторинг;
- согласование фактических изменений с утвержденными;
- Услуги в области подтверждения достоверности.

Корректирующие средства контроля

- анализ после реализации.

Планирование на случай непредвиденных обстоятельств (аварийное восстановление и обеспечение непрерывности бизнеса)

Планирование на случай непредвиденных обстоятельств обычно включает:

1) **Аварийное восстановление**, то есть процесс возобновления нормальных операций по обработке информации после возникновения серьезного сбоя, вызванного стихийными бедствиями (например, затопление, пожар или землетрясение). Требует резервных помещений и мощностей.

2) **Непрерывность бизнеса** – продолжение бизнеса другими способами в течение периода, когда компьютерная обработка данных недоступна или затруднена (например, из-за случайных (вирусы) или преднамеренных (взлом) вторжений).

Важно иметь:

- всеобъемлющий и актуальный (тестируется не реже одного раза в год) **План аварийного восстановления**, который описывает конкретные шаги, специалистов и ресурсы, необходимые для восстановления критически важного бизнес-процесса, и предусматривает
  - **Резервное копирование и ротацию за пределами объекта**.

Практические советы по проведению аудита общие средства контроля в ИТ-сфере

Проверьте политики и процедуры для общих средств контроля в ИТ-сфере

В случае их отсутствия

- *Определите соответствующие критерии аудита и*
- *Выработайте рекомендации по их внедрению в соответствии с приемлемой нормативной базой (например, ISO 27001/27002)*

Если они существуют, но имеют некоторые недостатки

- *Выработайте рекомендации по их улучшению*

Если они существуют и соответствуют всем требованиям

- *Используйте их в качестве критерия при оценке средств контроля*

Проверьте систему управления рисками (RMS)

Если RMS не разработана и не внедрена

- *Выработайте рекомендации по внедрению Стратегии и Методологии управления рисками*
- *Рекомендуйте создание Реестра рисков*

Если RMS существует, но имеет недостатки в структуре или функциониро-вании

- *Рекомендуйте соответствующие улучшения (например, регулярно, не реже одного раза в год, обновлять Реестр рисков)*

Если RMS надлежащим образом разработана, внедрена и функционирует

- *Используйте ее для оценки рисков при проведении аудита*

Практические советы по проведению аудита общих средств контроля в ИТ-сфере

Проверьте информацию о сотрудниках (должностная инструкция, квалификация, численность)

Правила систематизации

- *Можно порекомендовать Департаменту информационных технологий улучшить Правила в части адекватности: описания должности, требуемых квалификаций и компетенций, правильного распределения обязанностей и т.д.*

Комплектование рабочих мест и обучение ИТ-специалистов

- *Совершенствование политики и практики трудоустройства, удержания и обучения сотрудников в Департаменте информационных технологий*

Сотрудник по вопросам информационной безопасности и сотрудник по защите персональных данных

- *Назначение сотрудника по вопросам информационной безопасности и сотрудника по защите персональных данных*
- *Необходимые допуски ИТ-специалистам для обработки персональных данных*

Проверьте разделение обязанностей

Если разделения не существует или оно имеет недостатки

- *Можно рекомендовать, чтобы определенные обязанности (например, системных аналитиков, программистов, операторов, библиотекарей файлов и других) возлагались на разных людей*

Если разделение существует, но имеет недостатки в структуре или функционировании

- *Можно рекомендовать, чтобы системные аналитики и программисты не имели доступа к работе центра обработки данных, производственным программам или файлам данных / Операторы не имели обязанностей по проектированию систем, либо возможности вносить изменения в программы*

Проверьте наличие компенсирующего контроля

- *Можно рекомендовать внедрение или улучшение эффективного надзора, контроля компьютерных журналов или библиотек*

Практические советы по проведению аудита общих средств контроля в ИТ-сфере

Проверьте средства контроля физического доступа и параметров окружающей среды

Средства контроля физическо-го доступа

- *Можно рекомендовать, например, внедрение и/или обновление: Систем контроля доступа, например, контроль с помощью считывателей карт; реестра ИТ-ресурсов; прав физического доступа и схемы защитных мер для контроля физического доступа или соответствующей документации, а также системы контроля перемещений (выдачи и возврата) оборудования и носителей*

Средства контроля окружающей среды

- *Можно рекомендовать, например, внедрение или правильное использование и обслуживание системы контроля температуры и влажности или системы пожаротушения (газообразной, не водяной) и т.д.*

Проверьте план на случай непредвиденных обстоятельств

План преодоления последствий аварийной ситуации

- *Можно рекомендовать, например, разработку всеобъемлющего и актуального Плана (регулярно обновляемого)*

Анализ влияния на бизнес

- *Должен быть выполнен и быть комплексным*

Периодическо-е резервное копирование и ротация вне помещений

- *Можно рекомендовать, например, периодически выполнять резервное копирование важных данных и программ*
- *и хранить их в соответствующем месте вне офиса.*

Практические советы по проведению аудита общих средств контроля в ИТ-сфере

Проверьте логические элементы управления доступом

Проверьте, применяется ли подробная Процедура управления доступом пользователей;

Проведите проверку Системы управления учетными записями пользователей (управляющей разрешениями доступа пользователей и контролирующей права доступа к файлам, системам и сервисам) на предмет того, правильно ли добавляются новые учетные записи и назначаются только авторизованным пользователям, своевременно ли удаляются устаревшие и неиспользуемые учетные записи;

Проведите проверку матриц контроля доступа — ограничивают ли таблицы авторизованных пользователей или устройств доступ к пользователям или физическим устройствам, которые по логике должны иметь доступ;

Изучите системные журналы действий, требующих тщательного изучения, таких как повторные неудачные попытки входа в систему и использование мощных служебных программ;

Проверьте, проводятся ли регулярные проверки Сотрудником по вопросам информационной безопасности и Сотрудником по защите персональных данных в журналах доступа к системе попыток доступа, особенно неудачных, и использования мощных служебных программ;

Особое внимание уделите лицам с правами и привилегиями администратора и проверьте, регулярно ли контролируется подход администратора и группы «Администраторы»;

Проверьте, используется ли автоматический выход из системы (отключение) неактивного терминала данных, чтобы предотвратить просмотр конфиденциальных данных на автоматическом терминале данных;

Проверьте, отделена ли сеть Wi-Fi, открытая для использования посторонними лицами (например, внешними посетителями), от внутренней сети;

Убедитесь, что административная панель для управления контентом и настройки системы недоступна напрямую через Интернет (удаленное обслуживание выполняется через VPN);

Убедитесь, что в случае удаленного доступа установлено VPN-соединение с обязательной аутентификацией авторизованного лица;

Практические советы по проведению аудита общих средств контроля в ИТ-сфере

Проверьте логические элементы управления доступом

Проверьте, обеспечивается ли защита внутренней сети путем ограничения доступа в Интернет с помощью блокировки вспомогательных сервисов через брандмауэр, и ознакомьтесь с его отчетами об использовании Интернета в масштабах всей организации, необычных схемах использования и попытках проникновения в систему.

Для защиты паролей от кражи делайте проверки мер безопасности, например:
- часто меняйте пароли (устанавливая относительно короткий максимальный срок хранения);
- устанавливайте обязательный минимальный срок хранения, чтобы пользователи не могли быстро изменить свои пароли обратно на их старые и удобные значения;
- сохраняйте старые пароли для предотвращения их использования;
- пароли не должны отображаться на экране;
- устанавливайте минимальную длину пароля и используйте оптимальные пароли (генерируемые случайным образом) восьмизначных (или более длинных) комбинаций цифр, прописных и строчных букв и специальных символов (не содержащих слов или фраз).

Проверьте использование шифрования, особенно:
- меры шифрования для защиты мобильных рабочих станций и носителей для мобильного хранения персональных данных (ноутбук, USB, внешние жесткие диски, CD-ROM, DVD и т.д.);
- использование последней версии криптографического протокола (TLS, заменяющего SSL) на веб-страницах;
- шифрование резервных копий с персональными данными;
- передачу конфиденциальных данных через VPN с использованием шифрования;
- методы шифрования в управлении сетью Wi-Fi (например, WPA2 или WPA2-PSK).

Проверяйте применение контролируемого удаления документов для соблюдения ограничения доступа, путем уничтожения данных, когда они больше не используются (путем измельчения бумажных документов и стирания магнитных носителей).

Практические советы по проведению аудита общих средств контроля в ИТ-сфере

Проверьте средства контроля для выявления вредоносных программ

Убедитесь, что:

Внедрены **процедуры** и установлена **ответственность** за борьбу с вредоносными программами, а также существует **программа обучения и повышения уровня осведомленности** пользователей;

Используется **авторизованное программное обеспечение** и соблюдаются **лицензионные соглашения** (используются только чистые и сертифицированные копии программного обеспечения, условно-бесплатное программное обеспечение не используется, новое программное обеспечение проверяется антивирусным программным обеспечением);

Выполняется быстрая установка **самых последних патчей, исправлений и обновлений**, и обновления **тестируются перед установкой**;

Сетевые серверы имеют программное обеспечение для обнаружения и удаления или хранения вредоносных программ;

Вложения и загрузки электронной почты (и файлы на несанкционированных носителях или из небезопасных сетей) проверяются, **шлюзы безопасности электронной почты** имеют программное обеспечение для сканирования вложений;

Антивирусное программное обеспечение непрерывно отслеживает вирусы (или черви) и устраняет их, а также немедленно обновляется, как только появляется информация о новых угрозах;

Программное обеспечение и данные для критически важных систем регулярно пересматриваются.

Практические советы по проведению аудита общих средств контроля в ИТ-сфере

Проверьте процессы разработки систем

Убедитесь, что:
Концепция жизненного цикла разработки систем (SDLC) существует и используется:
Официальное предложение — исходя из оценки потребностей,

Технико-экономические обоснования,

Утверждение системы Руководящим комитетом по ИТ,

Проектирование системными аналитиками и разработки программистами,

В особенности, проверьте следующее:

- Тестирование было выполнено (и документально оформлено) во время разработки системы;
- Возникали ли проблемы во время конверсии;
- Обучение было проведено и документация существует;
- Существует ли мониторинг для обеспечения постоянной производительности и непрерывного совершенствования, а также проверки его результатов.

Проверьте процесс управления изменениями

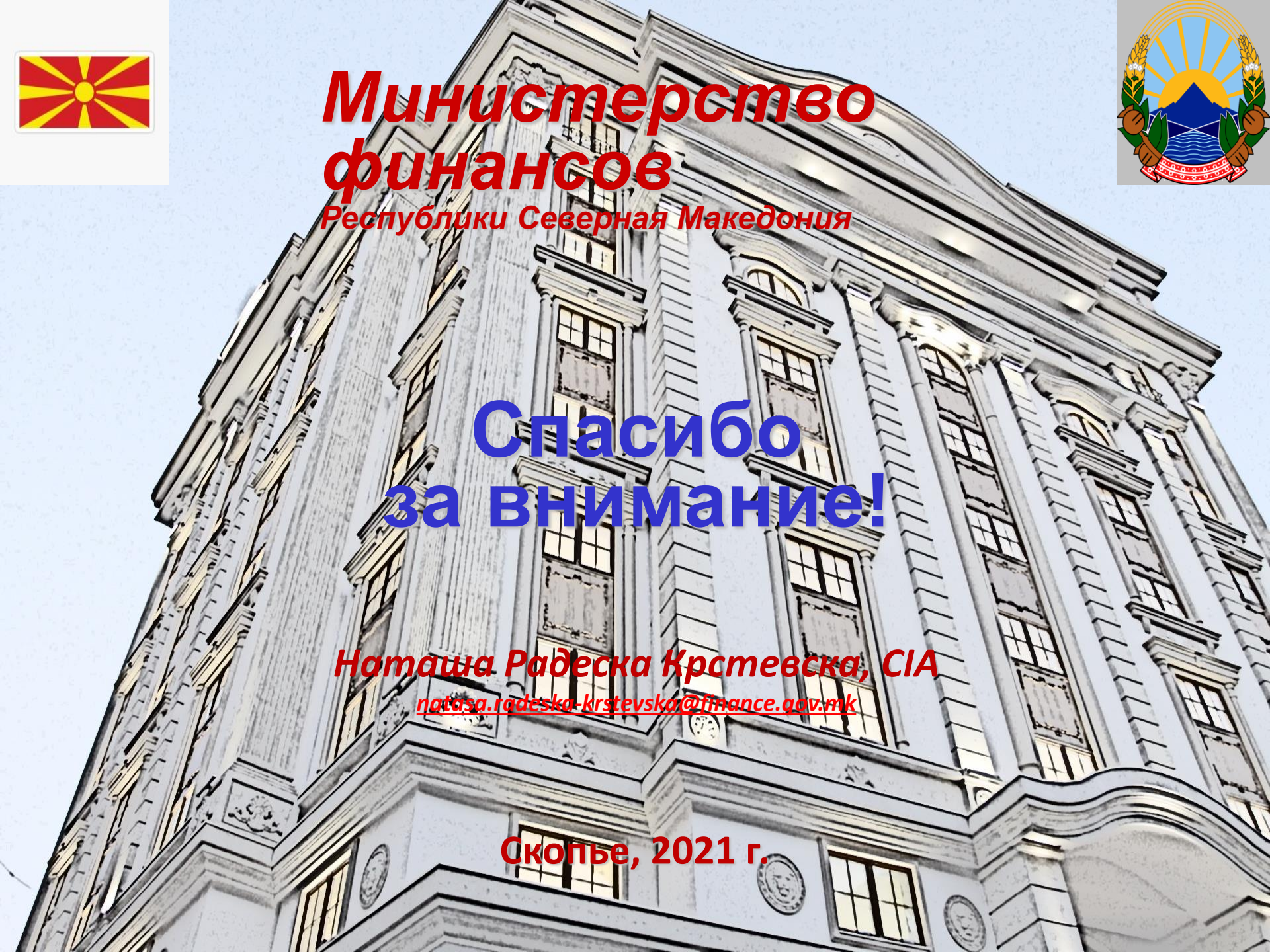
Был ли он определенным, повторяемым и предсказуемым.

Особенно важно убедиться, что

- Изменения тестируются в предпромышленной (тестовой) среде;
- Существуют разрешение на изменение, разделение обязанностей и ограничения, которые могут обновлять доступ к производственным данным и производственным программам;
- Существует мониторинг и Согласование фактических изменений с утвержденными изменениями.

Наличие Отчетов о полученном опыте, основанных на оценке следующих фактов:

- Насколько успешно были проведены изменения;
- Последовал ли процесс изменений;
- Существует ли расхождение между запланированными и осуществленными изменениями;
- Были ли соблюдены требования о соответствии.



Министерство финансов

Республики Северная Македония

Спасибо за внимание!

Наташа Радеска Крстевска, CIA

natasa.radeska-krstevska@finance.gov.mk

Скопье, 2021 г.