Приложение 2

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
(TERMS OF REFERENCE)

по проведению аудита информационных технологий Национального банка Таджикистана

Июнь, 2023
Душанбе, Таджикистан

I. Термины и определения

- Заказчик – Национальный банк Таджикистана, НБТ,
- Исполнитель – внешняя аудиторская организация
- Система управления информационной безопасности – часть общей системы управления организацией и совокупность внутренних организационно-распорядительных документов и ресурсов, необходимых для защиты активов Заказчика; обеспечивает осознанное принятие решений в области информационной безопасности (ИБ) через механизм управления бизнес-рисками при создании, внедрении, функционировании, мониторинге, анализе, поддержке и улучшении ИБ.

II. Обоснование

Целью аудита ИТ НБТ является проверка информационных систем, систем безопасности, а также процессов управления ИТ в целом на предмет соответствия как бизнес-процессам компании, так и международным стандартам. Такая проверка необходима, чтобы оценить правильность развития ИТ на основании международного опыта и утвердить принятые решения, документально их подтвердить.

Она позволяет направить деятельность ИТ-подразделения на достижение нового уровня развития ИТ в соответствии с международными стандартами. Проверка соответствия может помочь выявить неочевидные несоответствия в ИТ принятым стандартам и тем самым оправдать необходимость внесения изменений, а также определить, какие процессы или системы функционируют неэффективно и являются узкими местами для работы ИТ в целом.

Аудит ИТ позволяет оценить соответствие информационных систем требованиям бизнеса и построить долгосрочную стратегию развития информационных технологий. Также, поводом для проведения ИТ-аудита является необходимость выявить потенциальные риски и узкие места в ИТ-инфраструктуре. Только ИТ-аудит может подтвердить соответствие систем и бизнес-процессов международным стандартам, что является необходимым для любой компании, особенно банков.

III. Задачи аудита

Целью Банка при проведении системного аудита информационных систем и ИТ-инфраструктуры является получение разумной уверенности от стороннего аудитора в том, что:

- Информационные системы и данные Банка защищены и будут оставаться полными, интегрированными, актуальными и точными на протяжении всей обработки.
- Информационные активы/ресурсы Банка (аппаратное/программное обеспечение) защищены от несанкционированного доступа/использования/повреждения/изменения.
- Планирование непрерывности деятельности банка достаточно адекватно для обеспечения бесперебойного обслуживания клиентов, несмотря на перерывы в технических средствах в течение значительного периода времени.
- Сети банка должным образом обеспечены и защищены.
- Компьютерные операции банка осуществляются в контролируемой среде.
- Банк может получить независимую гарантию эффективности средств контроля, осуществляемых сторонними поставщиками технологических услуг (поставщик услуг по управлению объектами).
- Банк имеет соответствующие средства контроля на протяжении всего жизненного цикла разработки систем, управления проектами и деятельности по внедрению.
- Банк выполнил все требуемые законодательные нормы.

IV. Область аудита

Область аудита должна охватывать бизнес-процессы НБТ и соответствующие им информационные системы, программное обеспечение, системы связи и сетевую инфраструктуру, регламенты и протоколы управления для реализации ИТ-сервисов, предоставляемых внутренним пользователям Заказчика и внешним организациям (банки, микрофинансовые организации, страховые компании, государственные органы и ведомства, и т.д.).

В рамках проведения аудита Исполнитель оценивает текущее состояние системы управление информационной безопасностью и ИТ- инфраструктуры НБТ, а также выявить риски и возможности:

1. Оценка уязвимости инфраструктуры, относящейся к сети CBS, центру обработки данных, месту аварийного восстановления, вспомогательному офису CBS, головному офису, региональным офисам и филиалам и т. д.
2. Функционирование бэк-офиса CBS и центра обработки данных/DR. Аудит, охватывающий пользователя / справочную службу / параметры / доступ / внутренние исправления / управление изменениями и т. д.
3. Системный аудит основных банковских приложений, включая основное приложение. Широкие области, которые необходимо охватить, указаны в ***Приложении - I.***

4. Аудит сети, NMS (система мониторинга сети) и административный процесс с отчетом и рекомендациями. Широкие области, которые должны быть охвачены, указаны в ***Приложении - II***.
5. Отчет об управлении мощностями и настройке производительности всей архитектуры CBS с рекомендациями, если таковые имеются, по улучшению производительности и безопасности. Широкие области, которые должны быть охвачены, указаны в ***Приложении - III***.
6. Аудит процессов CBS с упором на критически важные области, такие как контроль паролей, контроль идентификаторов пользователей, безопасность операционной системы, контроль защиты от вредоносных программ, контроль проверки производителя, разделение обязанностей, ротация персонала, физическая безопасность, просмотр отчетов об исключениях / журналов аудита, политики непрерывности деятельности и тестирования и т. д.
7. Провести оценку уязвимости и системный аудит информационных систем стандартных приложений и устаревших приложений (либо интегрированных с Core Banking Solution, либо работающих автономно), таких как:
   - Платежные каналы, например, банкомат, мобильный банкинг, UPI;
   - RTGS, Reuters Dealing, CSD, 1C – Предприятия, NPCR, SWIFT и т.д.
8. Обзор текущих мер безопасности и рекомендации по их улучшению.
9. Аудит сайта аварийного восстановления (Disaster Recovery):
   - Проверка систем/контролей;
   - Оценка среды и процедур;
   - Оценка параметров управления;
   - Адекватность инфраструктуры (способность обрабатывать полный трафик);
   - Обзор резервных процедур;
   - Оценка контроля доступа.
10. Управление записями / Запись процессов и средств контроля:
    - Политика обращения с носителями, утилизации и транзита;
    - Периодический пересмотр уровней авторизации и списков рассылки;
    - Процедуры обращения, хранения и утилизации информации и носителей;
    - Хранение резервных копий носителей;
    - Защита записей от утери, уничтожения и фальсификации в соответствии с законодательными, нормативными, договорными и деловыми требованиями.
11. Оценка уязвимостей и тестирование на проникновение (VAPT) для всей ИТ-экосистемы, включая инфраструктуру информационной системы

банка (сетевые системы, устройства безопасности, серверы, базы данных, системы приложений, доступные через глобальную сеть, локальную сеть, а также с общедоступными IP-адресами, веб-сайтом банка и сервером электронной почты, размещенным у поставщика). Ожидается, что аудитор выявит существующие угрозы и уязвимости и предложит корректирующие решения и рекомендации по ним для снижения всех выявленных рисков с целью повышения безопасности информационных систем.

12. Комментарии аудитора/рекомендации по различным программам обучения, повышения знаний.
13. Разработать пакет рекомендаций для подготовки системы управления информационной безопасностью НБТ к сертификации по требованиям одного из международных стандартов информационной безопасности;
14. Провести оценку готовности Заказчика к сертификации системы управления информационной безопасностью, реализованной в НБТ, на соответствие одному из международных стандартов информационной безопасности;

Сбор данных:

Исполнитель должен провести фактический сбор соответствующих данных и информации, которые необходимы для оценки процесса системы управления информационной безопасности; и обеспечить согласованность данных и информации, и интерпретацию результатов.

Конфиденциальность:

Исполнитель должен сохранять конфиденциальность информации, собранной для проекта. Таким образом, для раскрытия данных или любой связанной с ними информации требуется согласие НБТ.

Интеллектуальная собственность:

Вся интеллектуальная собственность, включая исследования, отчеты или другие материалы, модели, электронные таблицы, принадлежат и остаются собственностью НБТ.

V. Обязанности Заказчика

Заказчик должен содействовать исполнителю в проведении аудита ИТ банка, предоставляя и обеспечивая следующее:

1) Координацию с соответствующими структурами НБТ (региональными отделениями, департаментами, управлениями, отделами НБТ и т.п.) относительно всей необходимой информации;
2) Техническую и административную поддержку работы, такую как организация встреч, интервью, презентаций и других сопутствующих мероприятий.

VI. Обязанности Исполнителя

Исполнитель обязан выполнить процедуры, указанные в главе IV. Исполнитель должен обладать следующим опытом и компетенцией:
1) иметь опыт в области оказания услуг проведении аудита ИТ-инфраструктуры;
2) должен обладать знаниями, опытом и возможностями для реализации настоящего проекта. В группе аудиторов должны быть специалисты хорошо владеющими знаниями в области систем управления информационной безопасности, международными стандартами информационной безопасности;
3) должен иметь возможность общения с сотрудниками НБТ и другими заинтересованными сторонами, а также иметь доступ к необходимым документам для выполнения услуг, в том числе к документации на английском языке по выбранному НБТ международному стандарту информационной безопасности.

VII. Сроки и результаты

Срок завершения работ по аудиту ИТ НБТ и представления аудиторского заключения определяется контрактом.

ПРИЛОЖЕНИЕ I

Объем системного аудита программного обеспечения Core Banking Solution ("CBS"):

- Элементы управления вводом;
- Управление обработкой;
- Управление выводом;
- Логический контроль доступа;
- Контролирует автоматизированную обработку/обновление записей, обзор или проверку важных расчетов, таких как процентные ставки, график погашения и т. д., обзор функционирования автоматизированных запланированных задач, разработку выходных отчетов, распространение отчетов и т. д;
- Возможность аудита как на стороне клиента, так и на стороне сервера, включая достаточность и точность регистрации событий, использование команд приглашения SQL, регистрацию на уровне базы данных всех других интерфейсов с другими приложениями и т.д;
- Степень параметризации;
- Функциональность;
- Внутренний контроль, встроенный на уровне прикладного программного обеспечения, на уровне базы данных, на стороне сервера и клиента;
- Процедуры резервного копирования/отката/восстановления и планирование на случай непредвиденных обстоятельств;
- Предложение о разделении ролей и обязанностей в отношении прикладного программного обеспечения для улучшения внутреннего контроля;
- Обзор документации по формальным стандартам именования, процесс разработки рабочих ролей, действий, групп и профилей, назначение, утверждение и периодический пересмотр профилей пользователей, назначение и использование доступа суперпользователя;
- Управляемость в отношении простоты настройки, отката транзакций, времени, необходимого для завершения дня, начала операций и процедур восстановления;
- Специальные замечания также могут быть сделаны по следующим пунктам:

  Жестко запрограммированные идентификатор пользователя и пароль, EDI, веб-сервер и другие интерфейсы на уровне сети, на уровне приложений. Процедуры восстановления и перезапуска. Достаточность и охват тестовых случаев UAT, обзор дефектов UAT и механизм отслеживания, развернутый поставщиком, и решение, включая повторное тестирование и приемка Обзор настроек, выполненных для программного обеспечения, и политика SDLC, которой следует такая настройка. Предлагаемая процедура управления изменениями во время преобразования, переноса данных, контроля версий и т. д.
- Предложите какие-либо инструменты или программы аудита для конкретных приложений;
- Обзор результатов тестов программного обеспечения и нагрузочное и стресс-тестирование ИТ-инфраструктуры, выполненное поставщиками;
- Адекватность журналов аудита и содержательных журналов;

- Соблюдение законодательных и законодательных требований;
- Настройка системной почты;
- Адекватность антивирусных мер в среде CBS;
- Адекватность защиты всех серверов (центр обработки данных и филиалы) и проверка применения последних исправлений, предоставленных различными поставщиками для известных уязвимостей, опубликованных CERT, SANS и т. д.;
- Помимо Системного аудита прикладного программного обеспечения, Системный аудит должен быть проведен в Центре обработки данных, на площадке аварийного восстановления, в головном офисе и региональном офисе.

ПРИЛОЖЕНИЕ II

Объем системного аудита компонентов сетевой инфраструктуры, сетей и безопасности приложений:

- Сканирование сети — оценка угроз и уязвимостей: это процесс измерения и приоритизации рисков, связанных с сетевыми и хост-системами и устройствами, позволяющий рационально планировать технологии и действия по управлению бизнес-рисками;
- Взлом пароля;
- Система обнаружения вторжений / Система предотвращения вторжений;
- Тестирование брандмауэр;
- Тестирование маршрутизатора;
- Тестирование на отказ в обслуживании (DOS);
- Распределенное тестирование DOS;
- Тестирование мер сдерживания;
- При выполнении теста на проникновение на серверах в реальной среде ISA должен обеспечить оптимальную производительность систем;
- Проверка программного обеспечения для мониторинга сети (NMS), установленного для мониторинга критически важных серверов всей сети, включая филиалы, для определения размера и т. д., для мониторинга сетевых компонентов LAN и WAN, управления неисправностями, управления производительностью сети, управления запасами, автоматического обнаружения. сетевых компонентов и т. д. NMS также реализована для упреждающего мониторинга, отчетности и создания отчетов о производительности основной банковской сети. Эти функциональные возможности должны быть проверены;
- Обзор сетевой инфраструктуры: сетевая инфраструктура в филиалах, офисе CBS-Project, центре обработки данных, сайте DR и NAP (сетевые точки агрегации);
- Анализ управления сетью. Необходимо пересмотреть ключевые аспекты управления, такие как стандарты для оборудования, приложений, планирования мощностей, производительности, отчетности, решения проблем, калькуляции и учета;
- Административная проверка сети:
  - Домены, которые необходимо проверить для эффективного администрирования сети;
  - Мониторинг структурированной кабельной системы и использования сети;
  - Оптимизация настройки;
  - Устранение узких мест;
  - Распределение полосы пропускания (требование/использование, особенно в часы пик для крупных/обслуживающих филиалов);
  - Стандартные отчеты и действия по устранению проблем;
  - Эффективность и безопасность передачи данных;
- Передача данных:
  - Размер пакета передаваемого сообщения;

- Скорость передачи сообщений. Безопасность пакетов сообщений, подлежащих передаче, независимо от того, защищены ли они от несанкционированного доступа. Адекватность процедур шифрования передаваемых данных;
- Протоколы передачи файлов FTP и SFTP.

- Аудит сетевой безопасности:
  - Необходимо пересмотреть меры физической и логической безопасности, инструменты и процессы, реализованные для защиты от несанкционированного проникновения в корпоративную сеть. Конфигурация брандмауэров и маршрутизаторов, эффективность системы обнаружения вторжений и/или автоматический аудит всех пользователей сети являются ключевыми областями, которые должны быть проверены. Проверить, обеспечена ли адекватная безопасность в различные сетевые подключения обеспечивают доступ к системе только авторизованным пользователям;
  - Проверить, включен ли удаленный вход в систему, и если да, то можно ли его идентифицировать по идентификаторам терминала/IP-адресам;
  - Проверить, не отключен ли удаленный вход через такие службы, как ftp, telnet и т.д;
  - В случае WAN (глобальные сети) обеспечивается ли безопасное обслуживание маршрутизатора для обеспечения эффективного системного администрирования;
  - Основное внимание следует уделить обнаружению уязвимостей системы, возникающих из-за множественных уровней доступа. Должны использоваться стандартные инструменты для сканирования различных точек входа в сеть и должен быть предоставлен исчерпывающий анализ целей безопасности. Область включает операционную систему, базы данных, брандмауэры, маршрутизаторы, устройства удаленного доступа и коммутаторы;
  - Проанализировать действия сетевого администратора/системного администратора и предлагать улучшения и элементы управления, если таковые требуются;
- Аудит устройств безопасности:
  - Конфигурация, наборы политик/правил, подписи, проверка, ведение журнала, расположение, избыточность, ограничения портов, исправления и обновления, администрирование и управление;
  - Брандмауэры (Juniper/CISCO и FortiGATE);
  - Системы предотвращения сетевых вторжений;
  - Хост-системы обнаружения вторжений;
- Архитектура и размещение устройств безопасности:
  - Процессы управления изменениями — развертывание правил, политик и адекватность управления изменениями с помощью инструмента регистрации неисправностей;
  - Процессы управления инцидентами;
  - Документация;
  - Адекватность служб мониторинга/антифишинга;
  - Адекватность мониторинга безопасности;

- Процессы аварийного/аварийного переключения и тестирование процессов аварийного/аварийного переключения;

- Адекватность механизмов отчетности и эскалации;
- Управление исправлениями.

ПРИЛОЖЕНИЕ III

Объем системного аудита управления мощностью и настройки производительности

Целью аудита планирования и управления мощностями является оценка того, обеспечиваются ли удовлетворительные уровни обслуживания пользователям экономичным способом.
Обзор следующих функций, выполняемых департаментом ИТ Банка:

- Определение требований к уровню обслуживания;
- Анализ текущей мощности;
- Анализ доступности пропускной способности сети на пиковом уровне;
- Планирование будущего;
- Периодический анализ рабочих нагрузок и услуг;
- Измерение общего использования ресурсов;
- Определение процесса измерения входящей работы;
- Установление требований к уровню обслуживания по сравнению с производительностью.