«УТВЕРЖДЕНО»
ЗАО «Спитамен Банк»
от _____

Председатель Правления
Самандарзода Н. _____

ЗАО "Спитамен Банк"
734064, Р.Т., Душанбе,
ул. Бободжона Гафурова, 45.
Тел:+992(44)600-65-65
www.spitamenbank.tj,
tender@spitamen.com

Тендерная документация и техническое задание на проведение комплексного ИТ-аудита и аудита информационной безопасности для ЗАО «Спитамен Банк»

г.Душанбе - 2026

1. Термины, определения и сокращения.

Банк, Заказчик – Закрытое акционерное общество «Спитамен Банк».

Победитель Тендера – Участник, предложение которого признано наиболее соответствующим требованиям тендерной документации и выбранным Банком в установленном порядке.

Исполнитель – Победитель Тендера после заключения договора с Банком на оказание услуг.

Предмет закупки - товары, работы или услуги, которые приобретаются Заказчиком в рамках единой процедуры закупки.

Тендер - осуществление конкурентного отбора Участников с целью определения Победителя, который обеспечивает наилучшие условия поставки товаров, выполнения работ и оказания услуг для потребностей Заказчика.

Тендерная документация - комплект документов, который содержит сведения об условиях Тендера, в том числе о порядке его проведения, требованиях к Участникам, критериях определения Победителя и т.п.

Тендерные предложения - предложения касательно предмета закупки или его части, которые Участники подают Заказчику в соответствии с требованиями Тендерной документации.

Тендерная комиссия - коллегиальный орган, состоящий из сотрудников Банка, которые назначены ответственными за организацию и проведение процедур закупки.

Участник – юридическое лицо, подавшее или намеренное подать тендерное предложение в рамках настоящего Тендера.

ИТ – Информационные технологии

ИБ – Информационная безопасность

ISO/IEC 27001 - Международный стандарт ISMS / compliance

NIST Cybersecurity Framework - рекомендации и структура работы по управлению киберрисками

COBIT - рекомендации и структура работы для IT governance

CIS Controls - Практический security controls framework / baseline

2. Предмет тендера.

Настоящее техническое задание определяет требования ЗАО «Спитамен Банк» (далее - «Банк» или «Заказчик») к закупке услуг по проведению комплексного ИТ-аудита и аудита информационной безопасности Банка с привлечением международной аудиторской компании, международной консалтинговой организации, либо признанной ИТ/ИБ-компании, обладающей подтвержденным опытом выполнения аналогичных работ в банковском секторе.

Документ предназначен для использования в рамках закупочной/тендерной процедуры и может быть направлен потенциальным участникам как запрос предложений (RFP / Request for Proposal). Техническое задание описывает ожидаемый объем работ, требования к результатам, общие требования к Исполнителю, порядок взаимодействия и состав материалов, которые должны быть представлены по итогам проекта.

ТЗ подготовлено для комплексной внешней оценки Банка в связи с регуляторными требованиями, необходимостью независимой оценки зрелости ИТ и ИБ, а также подготовкой к последующему формальному соответствию и/или сертификации по применимым международным стандартам.

3. Техническое задание и спецификация:

Основная цель проекта - получить независимую, профессиональную и практически применимую оценку текущего состояния ИТ, информационной безопасности, киберустойчивости, технических контролей, управленческих процессов и соответствия Банка применимым требованиям национального регулирования и международных стандартов.

3.1. Ключевые задачи

- проверить полноту, зрелость и фактическое исполнение ИТ- и ИБ-процессов Банка;
- оценить соответствие текущего состояния требованиям применимых международных стандартов и фреймворков;
- провести техническую оценку защищенности инфраструктуры, приложений, цифровых каналов, внешнего периметра и критичных систем;
- оценить архитектуру ИТ и ИБ, включая зоны доверия, сегментацию, интеграции, API и потоки данных;
- оценить уровень готовности Банка к последующей сертификации или формальному соответствию по ключевым стандартам;
- сформировать реестр рисков, gap-analysis, целевое состояние, roadmap улучшений и план корректирующих мероприятий;
- выполнить анализ достаточности ресурсов ИТ и ИБ, включая персонал, процессы и технологии, с подготовкой отдельного аналитического вывода и рекомендаций;
- сформировать высокоуровневую стратегическую рамку развития информационной безопасности Банка на 3-5 лет, увязанную с результатами аудита, целевым состоянием, уровнем зрелости, рисками, roadmap и применимыми международными практиками;
- подготовить управленческую презентацию для Правления/руководства Банка и версию отчета для внешнего предоставления.

3.2. Принципы выполнения

Работы должны выполняться с учетом риск-ориентированного подхода, критичности банковских операций, непрерывности обслуживания клиентов, конфиденциальности данных, недопустимости несанкционированного влияния на продуктивные системы и необходимости получения доказательной базы, достаточной для обоснования выводов Исполнителя.

4. Нормативная и методологическая основа

Исполнитель должен учитывать применимые обязательные требования законодательства Республики Таджикистан, нормативных актов и требований Национального банка Таджикистана, банковского регулирования, норм о банковской тайне, персональных данных, коммерческой тайне и иных обязательных правил, применимых к деятельности Банка. Регуляторные требования описываются в предложении и отчетах на уровне, достаточном для оценки соответствия, без необходимости перечисления всех нормативных актов в настоящем ТЗ.

Международная методологическая основа аудита должна включать, не ограничиваясь, следующие стандарты, фреймворки и лучшие практики:

Область	Минимальная методологическая база
Управление ИБ и рисками	ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, NIST Cybersecurity Framework, NIST SP 800-53, CIS Controls
ИТ-управление и ИТ-сервис	COBIT 2019, ITIL 4, ISO/IEC 20000
Непрерывность и устойчивость	ISO 22301, принципы cyber resilience, практики BIA/BCP/DRP
Прикладная безопасность	OWASP ASVS, OWASP Top 10, OWASP API Security Top 10, практики secure SDLC/DevSecOps
Специализированные банковские области	SWIFT Customer Security Programme / Customer Security Controls Framework;
Технические проверки	признанные международные методологии, vulnerability assessment, configuration review, security architecture review

При наличии расхождений между обязательными требованиями регулятора и международными практиками приоритет имеют обязательные требования национального законодательства и регулятора, если иное письменно не согласовано Банком.

5. Общий охват аудита

Аудит должен охватывать Банк в целом, включая ИТ-управление, ИБ-управление, инфраструктуру, критичные банковские системы, цифровые каналы, процессинговую и платежную инфраструктуру, SWIFT, процессы эксплуатации, разработку, управление доступами, непрерывность, техническую защищенность и фактическое исполнение процедур.

В рамках проекта Исполнитель должен проверять не только наличие внутренних документов и формальное соответствие требованиям, но и фактическое исполнение процедур через интервью, evidence, выборки, системные выгрузки, журналы, демонстрации, техническую валидацию и сопоставление утвержденных правил с реальной практикой Банка.

5.1. Матрица ключевых направлений

Направление	Ожидаемый охват
IT Governance / IS Governance	Управление ИТ и ИБ, роли, комитеты, политики, зрелость, соответствие COBIT/ITIL/ISO
Архитектура ИТ и ИБ	Сетевая архитектура, сегментация, зоны доверия, интеграции, API, потоки данных, secure-by-design
Core Banking / АБС	Архитектура, доступы, журналы, изменения, администрирование, резервирование, интеграции
ДБО / Digital Channels	Интернет-банк, мобильный банк, API, клиентская аутентификация, fraud controls, OWASP-риски
SWIFT CSP	Отдельный gap-analysis по SWIFT CSP, обязательные и рекомендательные контроли
Карточная и платежная инфраструктура	Процессинг, банкоматы, POS, шлюзы, карточные данные, мониторинг, интеграции
IAM/PAM	Жизненный цикл доступов, привилегии, MFA, SoD, сервисные и

	подрядные учетные записи
SOC/SIEM/IR	Источники логов, use cases, корреляция, playbooks, SLA, расследование, forensic readiness
BCP/DRP/Cyber Resilience	BIA, RTO/RPO, DR-сайт, восстановление, кризисное управление, cyber recovery
Техническое тестирование	Внешний/внутренний pentest, VA, web/mobile/API testing, AD, Wi-Fi, VPN, конфигурации
Физическая безопасность	Дата-центр, серверные, резервная площадка, контроль доступа, видеонаблюдение, инженерные системы
Third-Party / Vendor Risk	ИТ-аутсорсинг, поставщики, SLA, доступы подрядчиков, субподрядчики, концентрационный риск
SDLC / DevSecOps	Secure coding, CI/CD, code review, SAST/DAST/SCA, release/change management
Data Protection / DLP	Классификация данных, DLP, шифрование, маскирование, персональные данные, банковская тайна
Backup & Recovery	Политики, расписания, immutable/offline backups, тесты восстановления, ransomware resilience
Endpoint / Network / Email Security	EDR/XDR, firewalls, IDS/IPS, WAF, SOAR, NAD, VPN, DMZ, SPF/DKIM/DMARC, collaboration security
External Attack Surface	Домены, поддомены, exposed assets, SSL/TLS, DNS
Филиалы и устройства самообслуживания	Выборочная проверка филиалов, банкоматов, POS/терминалов и киосков
Применимые технологии	Cloud/virtualization/containers, remote work, AI/RPA/models при фактическом использовании

6. Детализированные требования к аудиторским блокам

6.1. ИТ-управление, ИБ-управление и зрелость

Исполнитель должен оценить модель управления ИТ и ИБ, распределение ролей и ответственности, участие профильных комитетов, достаточность процессов контроля, связь ИТ/ИБ-процессов с операционными рисками, а также общий уровень зрелости Банка по доменам. Оценка зрелости должна выполняться с использованием COBIT 2019, CMMI-подхода, NIST CSF tiers или иной признанной международной maturity-модели.

Для каждого ключевого домена должны быть определены текущее состояние, целевое состояние / target state, выявленный gap, рекомендации по переходу, приоритеты, зависимости и ожидаемый эффект.

6.2. IT Service Management

Аудит ITSM должен включать процессы incident, problem, change, release и request management, SLA/OLA, service catalogue, service desk, knowledge base, мониторинг, отчетность и метрики качества ИТ-сервиса. Оценка должна выполняться с учетом ITIL 4 и ISO/IEC 20000, включая фактическую проверку исполнения процедур по выборкам и evidence.

6.3. Архитектурный анализ ИТ и ИБ

Исполнитель должен выполнить полный архитектурный анализ текущей ИТ- и ИБ-архитектуры Банка, включая сетевую архитектуру, сегментацию, зоны доверия, DMZ, perimeter security, remote access, архитектуру критичных приложений, интеграции, API, потоки данных, Active Directory / IAM, резервирование, мониторинг и журналирование. Особое внимание должно быть уделено принципам defense-in-depth, least privilege, segregation of duties и secure-by-design.

6.4. Core Banking / АБС и ключевые банковские приложения

Отдельный блок должен охватывать Core Banking / АБС и ключевые банковские приложения: архитектуру, интеграции, параметры безопасности, управление доступами, журналы, изменения, резервирование, эксплуатационные процедуры, права администраторов и пользователей, а также ИТ/ИБ-контроли вокруг критичных операций. Функциональный аудит банковских операций не является самостоятельной целью, однако ИТ/ИБ-контроли, влияющие на критичные операции, должны быть оценены.

6.5. ДБО, цифровые каналы и API

Блок ДБО / Digital Channels должен охватывать интернет-банкинг, мобильный банкинг, клиентскую аутентификацию, безопасность сессий, fraud controls, защиту от OWASP-рисков, мониторинг, инциденты, эксплуатационные процессы и интеграции. Отдельно должен быть проведен API / Integration Security аудит: API gateway, внешние и внутренние интеграции, аутентификация, авторизация, шифрование, rate limiting, журналирование, управление ключами и защита от OWASP API Top 10.

6.6. SWIFT CSP

SWIFT Customer Security Programme / Customer Security Controls Framework должен быть выделен как отдельный специализированный блок. Исполнитель должен оценить SWIFT-инфраструктуру, архитектуру, зоны безопасности, управление доступами, журналирование, процедуры эксплуатации, соответствие обязательным и рекомендательным контролям SWIFT CSP, а также подготовить отдельный gap-analysis и рекомендации по устранению несоответствий.

6.7. Карточная, платежная инфраструктура и anti-fraud

Аудит должен включать отдельный блок карточной и платежной инфраструктуры: процессинг, банкоматы, POS-терминалы, платежные шлюзы, интеграции, безопасность карточных данных, операционные процессы, доступы, мониторинг, инциденты и зависимость от внешних поставщиков. Блок Fraud Monitoring / Anti-Fraud Controls должен охватывать правила выявления мошенничества, сценарии мониторинга, алерты, расследования, блокировки, интеграции с ДБО, картами, платежами, SOC/SIEM и операционными подразделениями, а также эффективность реагирования на fraud-события.

6.8. IAM/PAM и управление доступами

Исполнитель должен провести полный IAM/PAM аудит: жизненный цикл пользователей joiner/mover/leaver, роли и права, privileged access, администраторские и сервисные учетные записи, MFA, segregation of duties, периодический access review, доступы подрядчиков и внешних пользователей. Проверка должна охватывать фактическое соответствие прав утвержденным заявкам, ролям и бизнес-необходимости, включая критичные системы Банка.

6.9. SOC/SIEM, журналирование и реагирование на инциденты

Аудит SOC/SIEM/Incident Response должен включать архитектуру SOC/SIEM, источники логов, полноту журналирования, use cases, корреляционные правила, playbooks, SLA реагирования, эскалацию, расследование инцидентов, forensic readiness, сроки хранения логов, уведомления и постинцидентный анализ. Отдельно должен быть оценен Logging / Audit Trail / Time Synchronization: неизменяемость логов, централизованный сбор, интеграция с SIEM, NTP, audit trails и контроль доступа к логам.

6.10. BCP/DRP/Cyber Resilience и Backup & Recovery

Блок BCP/DRP/Cyber Resilience должен включать анализ BIA, RTO/RPO, планов непрерывности, аварийного восстановления, DR-сайта, кризисного управления, восстановления после киберинцидентов и фактической тестируемости процедур. Backup & Recovery выделяется отдельным техническим блоком и включает политики backup, расписания, покрытие критичных систем, хранение копий, immutable/offline backups, шифрование, тесты восстановления, защиту от ransomware и контроль доступа к backup-инфраструктуре.

6.11. Third-Party / Vendor Risk Management

Исполнитель должен оценить управление ИТ-аутсорсингом и третьими сторонами: облачные и телеком-провайдеры, процессинг, поставщики АБС/Core Banking, ДБО, SWIFT, SOC/SIEM, интеграторы, разработчики ПО, SLA, договорные требования по ИБ, доступы подрядчиков, субподрядчики и мониторинг рисков поставщиков. Отдельно должна быть оценена зависимость Банка от ключевых поставщиков, включая vendor lock-in, концентрационный риск, критичность сервисов, альтернативность и риски непрерывности.

6.12. SDLC / DevSecOps

Аудит SDLC / DevSecOps должен включать управление требованиями, разработку, тестирование, code review, secure coding, CI/CD, управление релизами, change management, контроль доступа разработчиков, разделение сред, управление исходным кодом, SAST/DAST/SCA, управление секретами в коде, безопасность API и управление уязвимостями приложений.

6.13. Infrastructure / Database / Hardening Review

Исполнитель должен проверить серверы, операционные системы, базы данных, middleware, сетевое оборудование, baseline configurations, hardening, системное и сетевое администрирование, журналы, резервирование, доступы, устаревшие версии и небезопасные протоколы. Проверка должна учитывать критичность систем и соответствие best practices по защищенной конфигурации.

6.14. Vulnerability & Patch Management

Аудит должен включать процесс выявления, классификации, приоритизации, устранения и повторной проверки уязвимостей, SLA, patch cycles, исключения, compensating controls, отчетность, метрики и связь с управлением рисками. Результаты технического vulnerability assessment должны быть сопоставлены с процессом управления уязвимостями и исправлениями.

6.15. Endpoint, Network, Email & Collaboration Security

Endpoint Security / EDR/XDR аудит должен охватывать рабочие станции и серверы, политики антивирусной защиты, EDR/XDR, контроль внешних устройств и USB, шифрование дисков, hardening конечных устройств, защиту администраторских рабочих станций, управление alert-ами

и интеграцию с SOC/SIEM.

Network & Perimeter Security аудит должен включать firewalls, IDS/IPS, WAF, NAD, NAC, VPN, DMZ, сегментацию, маршрутизацию, удаленный доступ, правила межсетевого экранирования, защиту внешнего периметра, сетевое журналирование и мониторинг.

Email & Collaboration Security аудит должен включать email gateway, anti-phishing controls, SPF/DKIM/DMARC, sandboxing, защиту вложений и ссылок, корпоративные мессенджеры и collaboration-платформы, DLP, архивирование, доступы, MFA и интеграцию с SOC/SIEM.

6.16. Data Protection / DLP и Cryptography / Key Management

Data Protection / DLP аудит должен охватывать классификацию данных, хранение, передачу, шифрование, маскирование, DLP, контроль каналов утечки, права доступа, защиту персональных данных, банковской тайны, коммерческой тайны и критичных данных Банка.

Cryptography / Key Management аудит должен включать криптографические политики, TLS-настройки, цифровые сертификаты, HSM при наличии, жизненный цикл ключей, генерацию, хранение, ротацию, отзыв, резервное копирование ключей, разграничение доступа, шифрование данных и защиту каналов связи. Вопросы электронной подписи, PKI и доверенной инфраструктуры отдельно не выделяются и оцениваются в данном блоке при применимости.

6.17. Физическая безопасность

Физическая безопасность должна быть оценена по дата-центру, серверным помещениям, резервным площадкам, зонам размещения сетевого оборудования, помещениям ИТ/ИБ-персонала, контролю физического доступа, видеонаблюдению, журналам посещений, сопровождению посетителей, охране, инженерным системам, пожарной безопасности и физической защите носителей информации.

6.18. Филиалы, ATM/терминалы и внешняя цифровая поверхность

Исполнитель должен провести выборочную проверку филиалов по риск-ориентированному подходу, включая ИТ-инфраструктуру филиалов, физическую безопасность, сетевые подключения, доступы, рабочие места, соблюдение ИТ/ИБ-процедур и взаимодействие с головным офисом. Перечень филиалов определяется Банком либо предлагается Исполнителем по критериям риска.

ATM / Terminal Security аудит должен охватывать банкоматы, POS/терминалы, киоски и иные устройства самообслуживания, сетевые подключения, hardening, обновления, физическую защиту, мониторинг, доступы, журналы, инциденты, эксплуатационные процедуры и зависимость от процессинговых или сервисных подрядчиков.

External Attack Surface аудит должен включать публичные домены, сайты, поддомены, IP-адреса, открытые сервисы, SSL/TLS, DNS, exposed assets, базовый OSINT, утечки учетных данных, бренд-риски, внешние зависимости и связь результатов с внешним penetration testing.

6.19. Социальная инженерия и оценка осведомленности персонала

Исполнитель должен провести оценку устойчивости Банка к сценариям социальной инженерии, включая phishing simulation, vishing, проверку реакции сотрудников, процедур эскалации, информирования ИБ-команды и эффективности awareness-программы. Любые сценарии

социальной инженерии, включая возможные физические, телефонные, электронные или иные сценарии, выполняются исключительно в пределах заранее согласованных Rules of Engagement, с определением допустимых методов, ограничений, целевых групп, сроков, контактных лиц, порядка остановки проверки и требований к конфиденциальности результатов. Результаты должны представляться в агрегированном виде с соблюдением конфиденциальности и недопущением необоснованного раскрытия персональных данных сотрудников.

6.20. Применимые блоки при наличии соответствующей инфраструктуры

Cloud / Virtualization / Container Security: облачные сервисы, виртуализация, гипервизоры, контейнеры, Kubernetes, IAM, сетевые настройки, журналы, резервирование, hardening и compliance - при фактическом использовании Банком.

Mobile Device / Remote Work / MDM/MAM, корпоративные мобильные устройства, VPN, MFA, удаленный доступ, политики, шифрование и защита корпоративных данных - при фактическом использовании соответствующих сценариев.

AI / RPA / Model Risk Security: модели, данные, доступы, RPA-боты, контроль изменений, журналирование, безопасность интеграций, риски ошибок и несанкционированных действий - при фактическом использовании таких технологий Банком.

6.21. Достаточность ресурсов и стратегическая рамка развития ИБ

Исполнитель должен оценить достаточность ресурсов Банка для обеспечения требуемого уровня ИТ, информационной безопасности и киберустойчивости. Оценка должна охватывать не только численность и компетенции персонала, но также зрелость процессов, достаточность технологических средств, организационную модель, распределение ролей, наличие ключевых функций контроля и способность Банка поддерживать устойчивое функционирование критичных ИТ- и ИБ-процессов.

Результатом оценки должен являться выделенный раздел итогового аудиторского отчета с оценкой достаточности ресурсов по направлениям «персонал - процессы - технологии», описанием выявленных дефицитов, влияния на риски Банка и практическими рекомендациями по устранению разрывов. Оценка ресурсной потребности для реализации roadmap указывается качественно, например Low / Medium / High effort, без финансовой оценки.

Исполнитель должен подготовить высокоуровневую стратегическую рамку развития информационной безопасности Банка на 3-5 лет, основанную на фактических результатах аудита, gap-analysis, оценке зрелости, целевом состоянии, реестре рисков, международных передовых практиках и приоритетах развития Банка. Документ должен определять стратегические направления, целевые ориентиры, ключевые инициативы и связь с roadmap, но не является утверждаемой корпоративной стратегией Банка, бюджетным документом или детальной программой внедрения.

7. Техническое тестирование и Rules of Engagement

Исполнитель должен включить в объем работ полный технический блок аудита ИБ: проверку сетевой инфраструктуры, Active Directory, Wi-Fi, VPN, почтовой безопасности, конфигураций серверов, баз данных, облачных или виртуализированных сред при наличии, а также критичных банковских систем.

До начала любых активных проверок Исполнитель обязан согласовать с Банком Rules of Engagement / План безопасного технического тестирования. Отдельный перечень инструментов тестирования в составе ТЗ не требуется; допустимые методы, ограничения и условия применения инструментов определяются в Rules of Engagement.

Элемент Rules of Engagement	Минимальное содержание
Объекты тестирования	Системы, IP-адреса, приложения, сегменты, среды, филиалы или устройства, разрешенные к тестированию
Окна работ	Допустимые временные интервалы, ограничения для продуктивных и критичных систем
Разрешенные и запрещенные действия	Допустимые методы, запрет destructive testing, DoS/DDoS, стресс-тестов и действий, способных нарушить работу систем без отдельного письменного согласования
Контакты и эскалация	Ответственные лица Банка и Исполнителя, канал экстренной связи, emergency stop procedure
Критичные уязвимости	Порядок незамедлительного рабочего уведомления проектной команды Банка без ожидания финального отчета
Логирование действий	Требования к фиксации действий Исполнителя, защите результатов и восстановлению штатного состояния после тестирования

8. Организация проекта

8.1. Срок и формат выполнения работ

Ожидаемый срок выполнения проекта - 3 месяца с даты начала работ, если иное не будет согласовано Банком. Участник в составе предложения должен представить календарный план в пределах указанного срока с этапами, ключевыми активностями, контрольными точками и результатами каждого этапа.

Формат выполнения работ - гибридный: часть работ проводится onsite на территории Банка, включая головной офис, дата-центр, резервную площадку, зоны физической безопасности и ключевые интервью; часть работ может выполняться удаленно через защищенные каналы и согласованный порядок обмена материалами.

8.2. Доступ к информации и системам

Ограниченный доступ через сопровождение сотрудников Банка: Исполнитель изучает материалы, системы, конфигурации и журналы только в присутствии или при сопровождении ответственных сотрудников Банка, без самостоятельного неконтролируемого доступа к продуктивным системам.

8.3. Коммуникации и встречи

Исполнитель должен провести kick-off meeting, согласовать рабочий график, обеспечивать регулярное информирование проектной команды Банка о ходе выполнения работ, статусе ключевых активностей, выявленных существенных вопросах и готовности промежуточных/итоговых материалов. Регулярные рабочие встречи проводятся с проектной командой Банка, а финальная презентация результатов - для руководства Банка / Правления /

профильного комитета.

Рабочее взаимодействие может осуществляться на русском и/или английском языке. Итоговые материалы по настоящей версии ТЗ должны быть подготовлены на русском языке. Английская версия ToR может быть подготовлена позднее после согласования русской редакции.

8.4. Промежуточные результаты

Поэтапная сдача результатов осуществляется умеренно и включает: стартовый план/календарный график работ, рабочие уведомления о критичных рисках при выявлении, проект отчета для обсуждения с Банком, финальный комплект документов, финальную презентацию и сессию передачи знаний. Формальная процедура приемки регулируется договором, а не настоящим ТЗ.

9. Требования к результатам и итоговым материалам

9.1. Состав deliverables

Результат	Требования к содержанию
Основной аудиторский отчет	Подробное описание текущего состояния, findings, рисков, gap-analysis, maturity assessment, рекомендаций, target state и плана корректирующих мероприятий
Реестр рисков и замечаний	Классификация Critical / High / Medium / Low, вероятность, влияние, бизнес-последствия, приоритет и рекомендуемые сроки устранения
Gap-analysis по стандартам	Отдельные матрицы по каждому ключевому стандарту: ISO 27001/27002/27005, ISO 22301, ISO 20000, COBIT 2019, ITIL 4, NIST CSF, NIST SP 800-53, CIS Controls, OWASP, SWIFT CSP
Maturity assessment	Оценка зрелости по доменам, текущий и целевой уровни, разрывы и меры повышения зрелости
Roadmap улучшений	Приоритизированная дорожная карта; период предлагает Исполнитель по итогам аудита; должны быть отражены зависимости, prerequisite actions и quick wins
План корректирующих мероприятий	Меры, приоритеты, сроки, зависимости, ожидаемый эффект, low/medium/high effort без назначения ответственных подразделений Банка
Управленческая презентация	Отдельная презентация для Правления/руководства Банка с ключевыми рисками, бизнес-влиянием, приоритетами и roadmap без излишней технической детализации
Версия отчета для внешнего предоставления	Версия отчета, пригодная для предоставления регулятору, внешним аудиторам или иным уполномоченным сторонам без раскрытия чувствительных технических деталей, IP-адресов, exploit evidence, учетных записей, конфигураций,

	логов и иной информации, которая может повысить риск для Банка
Технические приложения	Evidence, configuration review, скриншоты, таблицы, детали с учетом маскирования чувствительных данных
Knowledge transfer session	Сессия передачи знаний для ИТ, ИБ, риск-менеджмента, внутреннего аудита и иных заинтересованных подразделений
Раздел итогового отчета об оценке достаточности ресурсов	Оценка достаточности персонала, процессов и технологий ИТ/ИБ в составе основного аудиторского отчета; выявленные дефициты; влияние на риски; рекомендации по усилению ресурсной базы и качественная оценка требуемых усилий.
Высокоуровневая стратегическая рамка развития ИБ на 3-5 лет	Высокоуровневая стратегическая рамка, основанная на результатах аудита, gap-analysis, maturity assessment и target state; включает стратегические направления, целевые ориентиры, ключевые инициативы и связь с roadmap, но не является утверждаемой корпоративной стратегией, бюджетным документом или детальной программой внедрения.

9.2. Требования к качеству рекомендаций

Рекомендации Исполнителя должны быть конкретными, практически реализуемыми и применимыми к условиям Банка. Они должны быть связаны с выявленными рисками, gap-analysis, международными стандартами, целевым состоянием, зависимостями между мероприятиями, приоритетами и ожидаемым эффектом. Декларативные или общие рекомендации без практического пути реализации не должны рассматриваться как достаточные.

9.3. Форматы документов

Итоговые документы предоставляются в редактируемом и нередактируемом форматах, включая при необходимости Word / Excel / PowerPoint и PDF. Технические материалы и приложения предоставляются в согласованном защищенном электронном формате, а при необходимости — также на бумажном носителе с соблюдением режима конфиденциальности.

9.4. Evidence и приложения

Итоговые материалы должны включать подробные приложения с доказательной базой: перечень проверенных материалов, интервью, систем, выборок, gap-analysis, результаты технических проверок, скриншоты и иные evidence. Чувствительные данные, пароли, персональные данные, ключи, токены, внутренние IP-адреса и иная критичная информация должны маскироваться, если ее раскрытие в отчете не является необходимым.

10. Требования к Исполнителю и проектной команде

Исполнитель должен быть международной аудиторской или консалтинговой компанией, включая компании уровня Big Four, либо признанной международной или региональной ИТ/ИБ-компанией с подтвержденным опытом проведения комплексных ИТ-аудитов и аудитов ИБ в

банках и финансовых организациях.

10.1. Минимальный опыт

- не менее 7 лет подтвержденного опыта компании в области ИТ-аудита, ИБ-аудита, кибербезопасности или технологического консалтинга;
- не менее 5 комплексных проектов ИТ-аудита / ИБ-аудита в банках или финансовых организациях за последние 3 года;
- подтвержденный опыт работ по ISO/IEC 27001, COBIT, ITIL, SWIFT CSP, NIST CSF, BCP/DRP, техническому тестированию и оценке зрелости;
- ключевые эксперты проекта должны иметь, как правило, не менее 10 лет релевантного профессионального опыта по соответствующим направлениям.

10.2. Сертификации и роли

Проектная команда должна включать специалистов с релевантными сертификациями, такими как CISA, CISM, CISSP, CRISC, CGEIT, CDPSE, ISO/IEC 27001 Lead Auditor/Lead Implementer, COBIT, ITIL, OSCP/OSWE или аналогичные, PCI QSA / SWIFT CSP Assessor при наличии соответствующих блоков работ. На этапе предложения Участник представляет перечень сертификаций без обязательного раскрытия ФИО специалистов; копии действующих сертификатов и/или иные подтверждающие документы предоставляются по запросу Банка на этапе уточнения предложения, преддоговорных переговоров или перед заключением договора.

Минимальный состав ключевых ролей должен включать Project Manager, IT Audit Lead, Information Security Lead, Technical Security Testing Lead, Infrastructure / SOC Expert, BCP/DRP Expert, SWIFT CSP Expert, Core Banking / АБС Expert, Digital Channels Expert, а также специалистов по IAM/PAM, Network Security, Application Security, Vendor Risk и Physical Security при необходимости.

На этапе предложения Участник представляет состав проектной команды с указанием ролей, профессиональных профилей, релевантного опыта, сертификаций, ожидаемой загрузки, профилей / резюме ключевых экспертов и подтверждения их доступности для участия в проекте. Человеко-дни и численность команды остаются на усмотрение Исполнителя при условии обоснования достаточности команды для выполнения полного объема работ за 3 месяца.

10.3. Референсы

Исполнитель может представить сведения об аналогичных проектах и клиентских референсах только при наличии разрешения соответствующих клиентов и без раскрытия конфиденциальной информации. При отсутствии такого разрешения Исполнитель должен подтвердить релевантный опыт в обобщенном виде.

Отдельный развернутый раздел о независимости Исполнителя в ТЗ не включается; применяются стандартные закупочные требования о добросовестности, отсутствии конфликта интересов, раскрытии аффилированности, соблюдении конфиденциальности и недопустимости искажения результатов аудита.

11. Конфиденциальность, защита данных и обращение с материалами

Исполнитель обязан обеспечить строгий режим конфиденциальности и защиты данных, включая NDA, соблюдение банковской тайны, коммерческой тайны, персональных данных и требований регулятора. Передача информации третьим лицам без письменного согласия Банка не допускается.

Материалы аудита должны храниться в защищенной среде с контролем доступа и шифрованием при передаче и хранении. Доступ к evidence предоставляется только уполномоченным членам проектной команды Исполнителя. Результаты аудита, технические выгрузки, логи, скриншоты, конфигурации, exploit evidence и иные чувствительные материалы должны использоваться исключительно для целей проекта.

Данные Банка, банковская тайна, персональные данные, результаты аудита, evidence, технические выгрузки и иные чувствительные материалы не могут передаваться за пределы согласованной юрисдикции, защищенной среды или периметра, утвержденного Банком, без предварительного письменного согласия Банка. Отдельный запрет на использование публичных облаков, AI/LLM-инструментов и сторонних платформ в настоящем ТЗ не выделяется; такие вопросы покрываются общим режимом конфиденциальности и защиты данных.

После завершения проекта материалы должны быть возвращены Банку или уничтожены в порядке, предусмотренном договором и согласованным режимом обращения с evidence.

12. Требования к структуре предложения участника

Для сопоставимости предложений Участник должен представить предложение в структурированном виде. Критерии оценки и порядок выбора победителя определяются разделом 18 настоящей тендерной документации и применимыми внутренними процедурами Банка.

№	Раздел предложения
1	Резюме предложения и понимание целей проекта
2	Описание методологии аудита и используемой международной методологической базы
3	Детальный scope of work по направлениям, включая применимые и условные блоки
4	Подход к регуляторному compliance и международным стандартам
5	Подход к техническому тестированию, pentest, социальной инженерии и Rules of Engagement
6	Календарный план выполнения работ в пределах 3 месяцев
7	Проектная команда: роли, профили, опыт, сертификации, ожидаемая загрузка без обязательного указания ФИО
8	Релевантный банковский опыт и референсы при наличии разрешений клиентов
9	Перечень deliverables и форматы предоставления материалов
10	Финансовое предложение с указанием общей стоимости оказания услуг и разбивкой стоимости по основным этапам выполнения работ, включая подготовительный этап, аудит и анализ, техническое тестирование, подготовку отчетности, финальную презентацию и передачу итоговых материалов; детализация налогов, командировочных, onsite-расходов и иных сопутствующих расходов регулируется закупочной документацией и/или договором
11	Таблица соответствия требованиям ТЗ с указанием статуса: соответствует / частично соответствует / не соответствует, ссылки на раздел предложения и комментария

12	Подход к оценке достаточности ресурсов и подготовке высокоуровневой стратегической рамки развития ИБ на 3-5 лет

13. Приложения-шаблоны

Ниже приведены рекомендуемые структуры приложений, которые должны быть использованы или адаптированы Исполнителем при подготовке итоговых материалов. Форматы могут быть уточнены Исполнителем, но должны сохранять сопоставимость, проверяемость и применимость для Банка.

13.1. Приложение 1. Шаблон реестра рисков и замечаний

ID	Домен	Finding / замечание	Критичность	Вероятность	Бизнес-влияние	Рекомендация	Приоритет
R-001	IAM/PAM	[описание]	Critical/High/Medium/Low	[оценка]	[описание влияния]	[мера]	[срок/приоритет]
R-002	BCP/DRP	[описание]	Critical/High/Medium/Low	[оценка]	[описание влияния]	[мера]	[срок/приоритет]

13.2. Приложение 2. Шаблон gap-analysis по стандартам

Стандарт/контроль	Требование	Текущее состояние	Статус	Evidence	Gap	Рекомендация
ISO/IEC 27001 A.x	[требование]	[описание]	Соответствует/частично/не соответствует	[ссылка]	[gap]	[мера]
SWIFT CSP x.x	[контроль]	[описание]	Соответствует/частично/не соответствует	[ссылка]	[gap]	[мера]

13.3. Приложение 3. Шаблон roadmap улучшений

Инициатива	Связанные риски	Приоритет	Зависимости	Оценка усилий	Ожидаемый эффект	Период
[инициатива]	[ID рисков]	High/Medium/Low	[prerequisite actions]	Low/Medium/High	[эффект]	[предложенный Исполнителем период]
Quick win: [мера]	[ID рисков]	High	[нет/минимальные]	Low	[быстрое снижение риска]	0-3 мес. или иной период

13.4. Приложение 4. Шаблон плана корректирующих мероприятий

Мероприятие	Описание действия	Основание	Приоритет	Рекомендуемый срок	Зависимости	Примечание
[мера]	[конкретное действие]	[finding/gap]	[уровень]	[срок]	[зависимость]	Ответственные подразделения определяются Банком
[мера]	[конкретное действие]	[finding/gap]	[уровень]	[срок]	[зависимость]	[комментарий]

13.5. Приложение 5. Шаблон отчета по техническому тестированию

Раздел	Содержание
Объем тестирования	Системы, приложения, сегменты, периоды тестирования, ограничения Rules of Engagement
Методология	Классы примененных проверок и подходов без обязательного раскрытия полного инструментария
Выявленные уязвимости	Описание, критичность, доказательство, влияние, условия эксплуатации, рекомендации
Evidence	Скриншоты, технические подтверждения, логи и артефакты с маскированием чувствительных данных
Уведомления	Отдельная фиксация критичных рисков, о которых Банк был уведомлен в рабочем порядке

13.6. Приложение 6. Шаблон evidence register

ID evidence	Источник	Описание	Дата получения/проверки	Связанный finding	Уровень чувствительности/маскирование
E-001	[документ/система/интервью]	[описание]	[дата]	[ID]	[маскировано/не применимо]
E-002	[техническая выгрузка]	[описание]	[дата]	[ID]	[маскировано]

13.7. Приложение 7. Шаблон матрицы охвата аудита

Аудиторский блок	Системы/процессы	Стандарты	Evidence	Deliverables
IAM/PAM	AD, Core Banking, ДБО, SWIFT	ISO 27001, COBIT, NIST	[перечень]	Risk register, gap-analysis, report
BCP/DRP	DR-site, backup, critical systems	ISO 22301, NIST CSF	[перечень]	Maturity, roadmap, corrective actions

13.8. Приложение 8. Шаблон compliance matrix участника

№ требования ТЗ	Требование	Статус соответствия	Ссылка на раздел предложения	Комментарий участника
[раздел]	[текст требования]	Соответствует/частично/не соответствует	[раздел/страница]	[комментарий]
[раздел]	[текст требования]	Соответствует/частично/не соответствует	[раздел/страница]	[комментарий]

13.9. Приложение 9. Шаблон раздела итогового отчета об оценке достаточности ресурсов

Направление	Текущее состояние	Оценка достаточности	Выявленный дефицит/риск	Рекомендация
Персонал и компетенции	[описание]	Достаточно/частично/недостаточно	[дефицит]	[рекомендация]
Процессы и технологии	[описание]	Достаточно/частично/недостаточно	[дефицит]	[рекомендация]

13.10. Приложение 10. Шаблон высокоуровневой стратегической рамки развития ИБ на 3-5 лет

Рекомендуемая структура высокоуровневой стратегической рамки развития ИБ: стратегический контекст и цели; исходное состояние и ключевые риски; целевое состояние / target state; стратегические направления развития; ключевые инициативы на 3-5 лет; связь с roadmap; ожидаемый эффект; предпосылки и зависимости реализации. Документ не является утверждаемой корпоративной стратегией Банка, бюджетным документом или детальной программой внедрения.

Стратегическое направление	Целевое состояние	Ключевые инициативы	Горизонт
Governance ИБ	[target state]	[инициативы]	1-3 года / 3-5 лет
Технологическая защита и мониторинг	[target state]	[инициативы]	1-3 года / 3-5 лет
Культура ИБ и компетенции	[target state]	[инициативы]	1-3 года / 3-5 лет

14. Заключительные положения

Настоящее ТЗ определяет минимальный ожидаемый уровень охвата и качества услуг. Участник вправе предложить более зрелый, расширенный или уточненный подход, если он не сужает согласованный объем работ, не снижает требования к безопасности, конфиденциальности и

качеству результатов и соответствует целям Банка.

Проект считается завершенным после проведения финальной презентации, сессии передачи знаний, передачи полного комплекта итоговых документов и выполнения иных условий, установленных договором. Повторная проверка устранения замечаний / retest не включается в объем настоящего проекта, если Банк не примет отдельное решение о закупке такой услуги.

15. Подача тендерных предложений:

Тендерное предложение составляется на имя Банка и подается на фирменном бланке Участника, подписанном руководителем или уполномоченным лицом.

Тендерное предложение отправляется в заклеенном и запечатанном конверте с указанием названия, почтового адреса, контактных телефонов, других контактных данных или в электронном виде на адрес tender@spitamen.com:

«Тендер на проведение комплексного ИТ-аудита и аудита ИБ»

Адрес для подачи Тендерного предложения:

Тендерные предложения подаются по адресу: ЗАО «Спитамен Банк», 734064, Республика Таджикистан, г. Душанбе, ул. Бободжона Гафурова, 45, либо направляются на адрес электронной почты: tender@spitamen.com. Каждый Участник имеет право подать только одно тендерное предложение.

Тендерное предложение должно быть представлено на русском языке. Участник вправе дополнительно предоставить версию тендерного предложения или отдельных материалов на таджикском и/или английском языке. В случае расхождений между языковыми версиями приоритет имеет русская версия.

Тендерные предложения, оформленные с нарушением данных требований, к рассмотрению не принимаются.

16. Предельный срок подачи тендерного предложения.

Предельный срок подачи тендерных предложений — до 17:00 часов 1 июня 2026 года по времени г. Душанбе.

После окончания срока подачи Тендерных предложений Участников в Тендерную комиссию прием дополнительной информации к этим Тендерным предложениям не осуществляется.

Срок действия тендерного предложения должен составлять не менее 90 дней с даты предельного срока подачи тендерного предложения.

17. Место вскрытия тендерных предложений.

Вскрытие тендерных предложений осуществляется по адресу: 734064, г. Душанбе, ул. Бободжона Гафурова, 45, в здании Головного офиса Банка.

18. Выбор победителя Тендера.

Тендерное предложение может быть отклонено в случае, если Участник не соответствует квалификационным критериям или не отвечает требованиям Тендерной документации.

Принятие окончательного решения о победителе Тендера происходит на закрытом заседании Тендерной комиссии без приглашения Участников тендера.

При определении Победителя используются следующие критерии:
- Стоимость предложений.
- Квалификация и опыт проведения комплексного ИТ-аудита и аудита ИБ.
- Сроки оказания услуг.
- Клиентский портфель организаций-участников, отзывы от клиентов, рекомендательные письма.

19. Информация для контактов:

Для получения дополнительной информации по условиям/проведению Тендера следует обращаться к уполномоченному сотруднику Банка: телефон (44)-640-65-65, e-mail: tender@spitamen.com

Приложение:

1. Квалификационная заявка.
2.

Приложение № 1.

1. Квалификационная заявка.

Общая информация:		
1	Полное наименование	
2	Вид собственности	
3	Место регистрации	
4	Дата регистрации	
5	ИНН (Индивидуальный налоговый номер)	
6	Номер свидетельства плательщика НДС	
7	Ф.И.О., должность и основание полномочий руководителя	
8	Ф.И.О. и должность главного бухгалтера / финансового ответственного лица	
9	Ф.И.О., должность и основание полномочий лица, имеющего право подписи	
Контактная информация:		
1	Юридический адрес	
2	Фактический адрес	
3	Телефон	
4	Факс	
5	E-mail	
6	Интернет сайт	
Квалификационные данные Участника Тендера		

Лицензии, сертификаты:		
1	Наличие лицензии на осуществление определённого вида хозяйственной деятельности, являющегося предметом тендера (в случае, если такая деятельность подлежит лицензированию в соответствии с законодательством Республики Таджикистан), приложить копии	
2	Профессиональные сертификаты, аккредитации, партнерские статусы и иные подтверждения квалификации, применимые к предмету тендера	
Опыт работы по виду деятельности, являющимся предметом тендера:		
1	Общий период работы на рынке, лет	
2	Период работы по данному виду деятельности, лет	
3	Общее количество контрактов, шт. (допускается указание ориентировочного количества)	
4	Общая сумма контрактов, долл. (допускается указание ориентировочной суммы)	
Дополнительная информация:		
1	Основные направления деятельности компании	
2	Краткое описание инфраструктуры компании	
3	Количество сотрудников в штате компании, чел.	
4	Количество сотрудников, которые имеют необходимую квалификацию, для качественного выполнения заказа, чел.	
5	Сотрудник компании, у которого можно получить информацию по вопросам, связанным с предоставленной документацией (указать Ф.И.О. и конт. тел.)	
Отсутствие претензий со стороны государственных органов (Нет / Да; если "Да" - указать детали):		
1	Наличие неисполненных предписаний судебного органа	
2	Нахождение компании в процессе ликвидации, реорганизации или под процедурой банкротства	
3	Нахождение имущества под арестом либо в налоговом залоге	

4	Наличие возбужденных уголовных дел и неснятых судимостей в отношении руководителей	