Прошу изучить вложенные ПП от НБРК.

Также, помочь в формировании следующих процессов:

1. Разработка/актуализация матрицы доступов для АБИС Colvir;

2. Устранении замечании пентеста от компании Неташ.

3. Выявить иные задачи СБ.

Матрица доступа – таблица, отображающая правила разграничения доступа.

АБИС - Автоматизированная библиотечная информационная система - системы планирования ресурсов предприятий для библиотеки, которые используются для отслеживания библиотечных фондов, от их заказа и приобретения до выдачи посетителям библиотек.

Colvir - Core Banking System, a high-tech banking product and a universal solution for banks.

Пентест - тестирование на проникновение - метод оценки безопасности компьютерных систем или сетей средствами моделирования атаки злоумышленника.

Неташ - Netas Telekomunikasyon AS.

СБ - Служба Безопасности.

0) Постановление Правления Национального Банка Республики Казахстан

ПП - Постановление Правления

НБРК - Национальный Банк Республики Казахстан

1) "DOCUMENT" ПП НБ РК 12.11.2019

Об утверждении Правил формирования системы управления рисками и внутреннего контроля для банков второго уровня.

\* предоставление государственную регистрацию в Министерство Юстиции КЗ

\* размещение постановления на официальном интернет-ресурсе

\* направление копии на опубликование в Департамент Внешних Коммуникаций

Председатель НБ : Е. Досаев

Формирование системы управления рисками и внутреннего контроля банков второго уровня -> 31 августа 1995 год

Риски:

1) Риск информационных технологий - когда техника выходит из строя

2) Риск информационной безопасности - нарушение конфиденциальности

3) Уполномоченный коллегиальный орган банка - совет директоров, правление and so on

4) Репутационный риск - снижение показателей

5) Юридический риск - несоблюдение законодательства

6) Внутренний процесс оценки достаточности капитала - управление существенными рисками

7) Беззалоговый потребительский займ - банковский займ без условия о залоге на момент выдачи

8) Комплаенс-риск - вероятность возникновения потерь вследствии несоблюдения законодательства

9) Корпоративное управление - система взаимоотношений между работниками

10) Кредитный риск - невыполнение заемщиком или контрагентом своих обязательств в соответствии с условиями договора

11) Кредитоспособность - характеристика заемщика, оценить его возможность покрыть кредит

12) Кредитный договор - соглашение между банком и заемщиком

13) План финансирования на случай непредвиденных обстоятельств - совокупность процедур и плана действий для реагирования на снижение способности банка своевременно отвечать по своим обязательствам.

14) Подразделение-владелец защищаемой информации - подразделение банка, владелец информации, нарушение конфиденциальности, целостности или доступности которой приведет к убыткам для банка.

15) Критичный информационный актив - обеспечение информационной безопасности банков и организаций

16) Существенный риск - риск, реализация которого приведет к ухудшению финансовой устойчивости банка.

17) Конфликт интересов - ситуация при которой возникает конфликт между работниками банка и клиентами

18) Рыночный риск - возможные финансовые потери из-за рыночной ситуации

19) Операционный риск - возникновение потерь из-за неадекватных и недостаточных внутренних процессов, человеческих ресурсов и систем, или влияния внешних событий, за исключением стратегического риска и репутационного риска.

20) Внутренний процесс оценки достаточности ликвидности - набор процессов управления рисков ликвидности.

21) Риск ликвидности - вероятность возникновения финансовых потерь в результате неспособности банка выполнить свои обязательства в установленный срок без значительных убытков.

22) Политика - документ определяющий принципы, стандарты, стратегии.

23) Стратегический риск - возникновение рисков в ходе допущений ошибок при принятий решений, недостаточность в учете возможных опасностей.

24) Стресс-тестирование - метод оценки потенциального влияния исключительных, но возможных событий на финансовое состояние банка.

25) Риск - вероятность того что события окажут негативное влияние на финансовую устойчивость банка.

26) Риск-культура - процессы, процедуры, внутренние правила банка направленные на понимание, принятие, управление и контроль за рисками с целью минимизации их влияния на финансовое состояние банка, этические нормы и стандарты профессиональной деятельности организационной культуры.

27) Риск-профиль - совокупность видов риска и иных сведений, характеризирующие степень подверженности банка рискам.

28) Заявление риск-аппетита - утверждаемый советом директоров банка документ, описывающий агрегированный уровень существенных рисков.

29) Обработка риска - процесс выбора и реализации мер по изменению рисков.

30) Реестр рисков - структурированный перечень рисков, содержащий критерии и причины возникновения рисков, вероятность их возникновения, воздействие (ущерб), приоритет и способы обработки риска.

31) Уполномоченный орган - государственный орган, осуществляющий государственное регулирование, контроль и надзор финансового рынка и финансовых организаций.

32) Организационная структура - документ устанавливающий количественный состав, систему органов правления, подразделения банка, структуру подчиненности.

Бизнес модель банка - это совокупность выбранной стратегии, продуктов, процессов планирования, обеспечивающих конкурентоспособность и достаточный уровень доходности.

Совет директоров банка обеспечивает наличие системы управления непрерывностью деятельности банка, которая соответствует текущей рыночной ситуации, стратегии, объему активов, уровню сложности операций банка.

YELLOW:

0) обеспечение информационной безопасности;

1) 5) определяет группу наблюдателей (контролеров тестирования) из числа работников банка, ответственных за разработку плана (планов) по обеспечению непрерывности и (или) восстановлению деятельности, работников, осуществляющих внутренний контроль, и в случае необходимости, независимых специалистов из организаций, специализирующихся на оказании консультационных услуг в сфере обеспечения непрерывности деятельности и информационной безопасности банка. Группа наблюдателей (контролеров тестирования) осуществляет:

\* контроль выполнения каждого теста;

\* оценку результатов тестирования;

\* составление протокола о проведении тестов, его результатах и отзывах, включая необходимые корректирующие действия;

\* согласование протокола с руководителями подразделений банка, задействованных в тестировании плана (планов) по обеспечению непрерывности и (или) восстановлению деятельности;

2) Банк создает структурное подразделение по информационной безопасности, в функции которого входит:

\*) проведение оценки рисков информационной безопасности;

\*) разработка мер по обработке рисков информационной безопасности и предоставление отчетности по их реализации в подразделение по управлению рисками;

\*) подготовка и предоставление отчетности о реализации существенных рисков информационной безопасности в подразделение рисков банка, а также об устранении их последствий;

\*) разработка планов мероприятий по реализации стратегии банка в части обеспечения информационной безопасности.

3) Подразделение по информационной безопасности разрабатывает план мероприятий по реализации стратегии банка в части обеспечения информационной безопасности, который раскрывает, но, не ограничиваясь, следующее:

\*) определение потребностей в ресурсах, в том числе определение бюджета, связанного с реализацией мер, направленных на управление рисками информационной безопасности;

\*) описание требуемых мероприятий в области информационной безопасности с указанием сроков и ответственных исполнителей за их реализацию.

4) В случае привлечения внешних подрядчиков на аутсорсинг для выполнения отдельных операций и (или) осуществления бизнес-процессов совет директоров банка обеспечивает наличие эффективных принципов и практик управления рисками, возникающими в результате привлечения внешних подрядчиков. Мероприятия по привлечению внешних подрядчиков включают:

\*) процедуры определения того, какие функции передаются на аутсорсинг и каким образом;

\*) процессы осуществления проверки благонадежности финансового состояния компании при выборе потенциальных контрагентов;

\*) надежные принципы заключения контрактов с внешними подрядчиками, учитывающие структуру их собственности, условий конфиденциальности и предусматривающие права на расторжение контрактов;

\*) программы управления и мониторинга рисков, связанных с заключением таких контрактов, учитывающие финансовое положение источника услуг;

\*) создание условий для осуществления эффективного контроля в банке и в организации, оказывающей услуги;

\*) разработку эффективных планов на случай возникновения непредвиденных обстоятельств;

\*) выполнение комплексных контрактов и (или) договоров об оказании услуг с четким распределением обязанностей между организацией, оказывающей услуги и банком.

2) "DOCUMENT" Требования рус 48\_реализация

Об утверждении Требований к обеспечению информационной безопасности банков и организаций, осуществляющих отдельные виды банковских операций, Правил и сроков предоставления информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах.

GREEN:

0) Банк, организация обеспечивают создание и функционирование системы управления информационной безопасностью, являющейся частью общей системы управления банка, организации, предназначенной для управления процессом обеспечения информационной безопасности.

1) Система управления информационной безопасностью обеспечивает защиту информационных активов банка, организации, допускающую минимальный уровень потенциального ущерба для бизнес-процессов банка, организации.

2) Банк, организация обеспечивают надлежащий уровень системы управления информационной безопасностью, ее развитие и улучшение.

3) Участниками системы управления информационной безопасностью банка, организации являются:

\*) орган управления;

\*) исполнительный орган;

\*) коллегиальный орган, уполномоченный принимать решения по задачам обеспечения информационной безопасности (далее – коллегиальный орган);

4) Банк, организация определяют возможность делегирования другим подразделениям следующих функций подразделения по информационной безопасности:

\*) внедрение и администрирование программно-технических средств, автоматизирующих процесс обеспечения информационной безопасности банка, организации – подразделению по информационным технологиям;

\*) организация и проведение мероприятий по обеспечению осведомленности работников банка, организации в вопросах информационной безопасности – подразделению по работе с персоналом;

\*) учет и обработка событий и инцидентов информационной безопасности, связанных с нарушениями состояния информационной безопасности – подразделению по безопасности или отдельно выделенному подразделению обработки инцидентов информационной безопасности, независимому от подразделения по информационным технологиям.

YELLOW:

0) Орган управления банка, организации утверждает политику информационной безопасности, которая определяет:

\*) цели, задачи и основные принципы построения системы управления информационной безопасностью;

\*) область действия системы управления информационной безопасностью;

\*) требования к доступу к создаваемой, хранимой и обрабатываемой информации в информационных системах банка, организации и мониторинг информации и доступа к ней;

\*) требования к осуществлению мониторинга деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности;

\*) требования к осуществлению сбора, консолидации и хранения информации об инцидентах информационной безопасности;

\*) требования к проведению анализа информации об инцидентах информационной безопасности;

\*) ответственность работников банка, организации за обеспечение информационной безопасности при исполнении возложенных на них функциональных обязанностей.

1) Орган управления банка, организации утверждает перечень защищаемой информации, включающий в том числе информацию о сведениях, составляющих служебную, коммерческую или иную охраняемую законом тайну (далее – защищаемая информация), и порядок работы с защищаемой информацией.

2) Исполнительный орган банка, организации утверждает внутренние документы, регламентирующие процесс управления информационной безопасностью, порядок и периодичность пересмотра которых определяется внутренними документами банка, организации.

3) Банк, организация создают коллегиальный орган, в состав которого входят представители подразделения по информационной безопасности, подразделения по управлению рисками информационной безопасности, подразделения по информационным технологиям, а также при необходимости представители других подразделений банка, организации. Руководителем коллегиального органа назначается руководитель исполнительного органа банка, организации либо член исполнительного органа банка, организации, курирующий деятельность подразделения по информационной безопасности.

4) Подразделение по информационной безопасности в целях обеспечения конфиденциальности, целостности и доступности информации банка, организации осуществляет следующие функции:

\*) организует систему управления информационной безопасностью, осуществляет координацию и контроль деятельности подразделений банка, организации по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности;

\*) разрабатывает политику информационной безопасности банка, организации;

\*) обеспечивает методологическую поддержку процесса обеспечения информационной безопасности банка, организации;

\*) осуществляет выбор, внедрение и применение методов, средств и механизмов управления, обеспечения и контроля информационной безопасности банка, организации, в рамках своих полномочий;

\*) осуществляет сбор, консолидацию, хранение и обработку информации об инцидентах информационной безопасности;

\*) осуществляет анализ информации об инцидентах информационной безопасности;

\*) подготавливает предложения для принятия коллегиальным органом решения по вопросам информационной безопасности;

\*) обеспечивает внедрение, надлежащее функционирование программно-технических средств, автоматизирующих процесс обеспечения информационной безопасности банка, организации, а также предоставление доступа к ним;

\*) определяет ограничения по использованию привилегированных учетных записей;

\*) организует и проводит мероприятия по обеспечению осведомленности работников банка, организации в вопросах информационной безопасности;

\*) осуществляет мониторинг состояния системы управления информационной безопасностью банка, организации;

\*) осуществляет информирование руководства банка, организации о состоянии системы управления информационной безопасностью банка, организации.

5) Банк, организация определяют возможность возложения на подразделения по информационной безопасности функций по обеспечению технической безопасности. Подразделение по информационной безопасности не осуществляет функции, влекущие конфликт интересов с их основными функциями.

\*остановился 16 пункт #9-page\*

3) "DOCUMENT" НПА №200.rus

Об утверждении Требований к организационным мерам и программно-техническим средствам, обеспечивающим доступ в платежные системы.

4) "DOCUMENT" v2000021685.23-11-2020.rus

Об утверждении Правил оценки уровня защищенности от угроз информационной безопасности

Уровни защищенности.

5) "DOCUMENT" № 34\_2016

Об утверждении Требований к безопасности и беспрерывности работы информационных систем банков и организаций, осуществляющих отдельные виды банковских операций

\*) управления платежными системами

\*) электронных банковских услуг в штатном