**Комьютеризированная система 1С***)*

*(1С Computerized system)*

**АНАЛИЗ РИСКОВ***(RISK ANALYSIS)*

**ИСТОРИЯ ИЗМЕНЕНИЙ** *(CHANGE HISTORY)*

|  |  |  |
| --- | --- | --- |
| **Версия** *(Version)* | **Дата** *(Date)* | **Описание изменений** *(Change Description)* |
| 1.0 | DD.MM.YYYY | Первый выпуск *(First Issue)* |

**НАПИСАНО** *(WRITTEN BY)*

|  |  |  |  |
| --- | --- | --- | --- |
| **Должность** *(Role)* | **Имя** *(Name)* | **Дата** *(Date)* | **Подпись** *(Signature)* |
| Специалист по валидации  (Validation Specialist) |  |  |  |

**РАССМОТРЕНО** *(REVIEWED BY)*

|  |  |  |  |
| --- | --- | --- | --- |
| Должность *(Role)* | Имя *(Name)* | Дата *(Date)* | Подпись *(Signature)* |
| Ключевой пользователь  (Key User) |  |  |  |
| Владелец системы  (System Owner) |  |  |  |

**УТВЕРЖДЕНО** *(APPROVED BY)*

|  |  |  |  |
| --- | --- | --- | --- |
| Должность *(Role)* | Имя *(Name)* | Дата *(Date)* | Подпись *(Signature)* |
| Владелец процесса  (Process Owner) |  |  |  |
| Обеспечение качества  (Quality Assurance) |  |  |  |

Содержание *(Table of Contents)*

1 ВВЕДЕНИЕ *(INTRODUCTION)* 4

1.1 ЦЕЛЬ *(PURPOSE)* 4

1.2 СФЕРА ПРИМЕНЕНИЯ *(SCOPE)* 4

1.2.1 Вне сферы применения (Out of the Scope) 4

1.3 Справочная документация *(Reference Documentation)* 5

1.4 ГЛОССАРИЙ *(GLOSSARY)* 6

2 ПОДХОД И СТРАТЕГИЯ АНАЛИЗА РИСКОВ *(RISK ANALYSIS STRATEGY AND APPROACH)* 7

2.1 ПРОЦЕДУРА АНАЛИЗА РИСКОВ *(RISK ANALYSIS PROCEDURE)* 8

2.1.1 Сценарий риска / потенциальный сбой и воздействие (Risk Scenario / Potential Failure and Effect) 10

2.1.2 Типология рисков (Risk Typology) 11

2.1.3 Причины возникновения риска (Risk Root Cause) 11

2.1.4 Влияние сбоев (степень воздействия) (Impacts of Failures (Severity)) 11

2.1.5 Возможность сбоев (вероятность) (Probability of Failure (Likelihood)) 12

2.1.6 Классы рисков (Risk Class) 13

2.1.7 Способность обнаруживать сбои (обнаруживаемость) (Ability to Detect Failures (Detectability)) 14

2.1.8 Оценка приоритета риска (Risk Priority Evaluation) 15

2.2 РЕКОМЕНДАЦИИ ДЛЯ ДЕЙСТВИЙ ПО СМЯГЧЕНИЮ РИСКОВ *(GUIDELINES FOR RISK MITIGATION ACTIONS)* 16

3 ВЛОЖЕНИЯ *(ATTACHMENTS)* 17

1. ВВЕДЕНИЕ *(INTRODUCTION)*
   1. ЦЕЛЬ *(PURPOSE)*

Данный документ описывает **анализ рисков (RA)** Комьютеризированная система 1С, которая установлена и используется в компании ООО «МАКИЗ-ФАРМА»(далее Компания). Система применяется для управления [Instrument Name RUS] (с/н [Instrument Code]).  
(The present document is the Risk Analysis (RA) of the 1С Computerized systemhereinafter) installed and operating in the [Department Name] of [Client Name] (from now on Company), [Site Name] site. The system is used for managing the [Instrument Name] (s/n [Instrument Code]) instrument.)

Цель данного документа — представить методологию и результаты анализа рисков, выполненного на функциональном уровне системы.  
(Purpose of the present document is to describe methodology and results of risk analysis executed at system’s functional level.)

* 1. СФЕРА ПРИМЕНЕНИЯ *(SCOPE)*

Данный документ относится к жизненному циклу валидации Комьютеризированная система 1С, которая установлена на рабочей станции [Workstation ID] в [Department Name RUS] Компании и управляет [Instrument Name RUS] (с/н [Instrument Code]).  
(This document applies to the validation life cycle of 1С Computerized systemSystem installed [on the Workstation ID] in the [Department Name] of Company and controlling the [Instrument Name] (s/n [Instrument Code]) instrument.)

* + 1. Вне сферы применения *(Out of the Scope)*

Валидация компьютеризированной системы, не включает действия по квалификации:   
(Computerized system validation does not include qualification of)

• Подключённых приборов или оборудования (Linked equipment or instruments)

• ИТ-инфраструктуры (IT infrastructure)

Вышеперечисленные действия по квалификации должны рассматриваться как предварительное условие для проведения действий по валидации, описанных в данном документе.  
(Such Qualification activities have to be considered a prerequisite for the Validation activities described in the current document.)

* 1. Справочная документация *(Reference Documentation)*

Cм. План валидации раздел 1.3  
(Ref. to Validation Plan § 1.3)

**Внутренняя документация** (Internal documents):

1. План валидации Комьютеризированная система 1С, PLN.PD.QUA.954.01  
   (Granulation line 1 GEA Validation Plan, PLN.PD.QUA.954.01)
2. Спецификации функциональных / пользовательских требований системы Комьютеризированная система 1С, URS.GEN.CTR.225.01  
   (Granulation line 1 GEA User Requirements / Functional Specifications, URS.GEN.CTR.225.01)
3. Спецификации конфигурации и дизайна системы Комьютеризированная система 1С, CSP.GEN.CTR.009.01  
   (Granulation line 1 GEA Configuration and Design Specifications, CSP.GEN.CTR.009.01)
   1. ГЛОССАРИЙ *(GLOSSARY)*

|  |  |
| --- | --- |
| 1С Computerized system | [System Name] (№ [System Code]) |
| CDS | Спецификации конфигурации и дизайна *(Configuration and Design Specifications)* |
| CFR | Свод федеральных нормативных актов *(Code of Federal Regulations)* |
| FRS | Спецификации функциональных / пользовательских требований  *(User requirements / functional specifications)* |
| GxP | Надлежащая **x** Практика, где **x** может быть*(****G****ood* ***x******P****ractice, where x can be)*  M = Производственная *(Manufacturing)*  L = Лабораторная *(Laboratory)*  C = Клиническая *(Clinical)*  D = Дистрибьюторская *(Distribution)* |
| № *(ID)* | Идентификатор *(Identification)* |
| RA | Анализ рисков *(Risk Analysis)* |
| RAS | Сценарий анализа рисков *(Risk Analysis Scenario)* |
| TRM | Матрица прослеживаемости *(Traceability Matrix)* |
| VP | План валидации *(Validation Plan)* |
| ВАЛИДАЦИЯ *(VALIDATION)* | Решение Совета Евразийской экономической комиссии от 3 ноября 2016 г. №77 об утверждении Правил надлежащей производственной практики Евразийского экономического союза» определяет валидацию как:  “Документально оформленные действия, дающие высокую степень уверенности в том, что методика, процесс, оборудование, материал, операция или система соответствуют заданным требованиям и их использование будет постоянно приводить к результатам, соответствующим заранее установленным критериям приемлемости***”*** *(FDA Guidelines on General Principles of Process Validation, Jan 2011 defines validation as:“The collection and evaluation of data, from the process design state through commercial production, which establishes scientific evidence that a process is capable of consistently delivering quality product”)* |
| ИТ *(IT)* | Информационные технологии *(Information Technology)* |
| Компания  *(Company)* | ООО «МАКИЗ-ФАРМА» *MAKIZ-PHARMA LLC* |
| Н/П *(N/A)* | Не применимо *(Not Applicable)* |
| СОП *(SOP)* | Стандартная операционная процедура *(Standard Operating Procedure)* |

1. ПОДХОД И СТРАТЕГИЯ АНАЛИЗА РИСКОВ *(RISK ANALYSIS STRATEGY AND APPROACH)*

Основной целью валидации компьютеризированной системы в фармацевтической отрасли является обеспечение потребителей высококачественным фармацевтическим продуктом.  
(The main target of the computerized system validation activities in the pharmaceutical field is to assure the end consumers on high quality of pharmaceutical products.)

Правильный план действий по управлению рисками позволяет сосредоточить внимание на действиях по валидации для большинства критически важных систем GMP, а также внутри каждой системы на ее наиболее важной части, для того чтобы:  
(A correct risk management activity plan allows focusing on validation activities for the most GMP critical systems and, within each system, on its most critical parts, in order to:)

• Выявить и определить приоритетность рисков, связанных с использованием системы  
(Identify and prioritize the risks associated with the system use)

• Определить соответствующие действия по уменьшению последствий  
(Identify the related mitigation actions)

• Оптимизировать работу по валидации и применению системы  
(Optimise validation effort and system utilisation)

Анализ рисков был сфокусирован на процессе, управляемом системой, и следующих аспектах, связанных с безопасностью, целостностью и прослеживаемостью данных, управляемых самой системой.  
(The Risk Analysis has been focused on the process managed by the system and the aspects related to the security, integrity and traceability of data managed by the system itself.)

* 1. ПРОЦЕДУРА АНАЛИЗА РИСКОВ *(RISK ANALYSIS PROCEDURE)*

Анализ рисков будет проводиться в соответствии с методологией, представленной на следующем рисунке (Рис *(Img)* 1).  
(The Risk Analysis will be conducted according to the methodology sketched in the following figure (Рис (Img) 1).)



Рис *(Img)* 1 Процедура анализа рисков *(Risk Analysis Procedure)*

Согласно приведённому выше рисунку, методология анализа рисков основана на следующих элементах, которые подробно описаны в данных разделах:  
(According to the above Figure, the Risk Analysis methodology is based on the following elements, which are described in detail in the next sections:)

• Возможные варианты риска/ потенциальный сбой и его эффект  
(Risk Scenario/ Potential failure and effect)

• Влияние сбоев (Тяжесть)  
(Impact of failures (Severity))

• Возможность сбоев (вероятность)  
(Probability of failures (Likelihood))

• Классификация рисков  
(Risk Class assignment)

• Способность обнаруживать сбои (обнаруживаемость)  
(Ability to detect failures (Detectability))

• Оценка приоритетности рисков  
(Risk Priority evaluation)

Процесс, управляемый системой и описанный в документе спецификации функциональных / пользовательских требований (см.), был разделён на следующие секторы, для которых были идентифицированы несколько возможных сценариев риска / потенциального сбоя и связанных с ним рисков:  
(The process managed by the system, and described in the User Requirements / Functional Specification (see), has been divided in the following macro-activities for which several risk scenario/potential failure and the associated risks were identified:)

• Безопасность системы и данных   
(System & Data security)

• Целостность данных  
(Data integrity)

• Прослеживаемость данных  
(Data traceability)

• Подготовка анализа  
(Analysis preparation)

• Выполнение анализа / Сбор данных  
(Analysis execution/Data acquisition)

• Оценка данных и печатанье отчёта  
(Data evaluation & report printing)

Для каждого возможного варианта рисков был применён анализ риска для определения «приоритета риска» по следующим показателям:  
(For every risk scenario the following variables of risk analysis have been evaluated in order to determine the related “Risk Priority”:)

• Тяжесть  
(Severity)

• Вероятность  
(Likelihood)

• Класс риска  
(Risk Class)

• Обнаруживаемость  
(Detectability)

В качестве окончательного результата анализа были определены приоритеты риска, и меры, которые должны быть выполнены или приведены в действие, чтобы уменьшить вероятность каждого из найденных рисков.  
(As a final output of the analysis, the Risk Priorities have been assigned and the measures to be performed or in place, in order to mitigate each identified risk, have been identified).

Вышеперечисленные переменные анализа описаны в следующих разделах.  
(The previously listed variables of analysis are described in the following sections.)

Результаты проведённого анализа рисков представлены во вложении 1 «Результаты анализа рисков».  
(The results of the performed risk analysis are reported in the Attachment 1 “Risk Analysis Results”.)

* + 1. Сценарий риска / потенциальный сбой и воздействие *(Risk Scenario / Potential Failure and Effect)*

Первым шагом анализа рисков является идентификация возможных сценариев риска, которые обозначают тип сбоев, каковые могут произойти (потенциальный сбой) и связанный с ним эффект (потенциальное воздействие сбоя).  
(The first step of the Risk Analysis is the identification of the risk scenario, which means the type of failures that could occur (Potential failure) and the related effect (Potential effect of failure).)

Каждый идентифицированный возможный сценарий риска кодируется идентификатором риска (RAN №), описанный ниже:  
(Each identified risk scenario is codified by a Risk ID (RAN ID) described below:)

**RAS.YYY**

Структура кодировки риска состоит из:  
(Risk code structure is made of:)

• RAS — указывает на сценарий анализа риска  
(RAS indicate Risk Analysis Scenario)

• YYY — это последовательное число  
(YYY is a progressive number)

Каждый возможный вариант риска / потенциального сбоя будет прослежен в документе «Матрица прослеживаемости» (None) в соответствии с требованиями.  
(Each Risk Scenario/Potential Failure will be traced in the Traceability Matrix document (None) against the related requirements.)

* + 1. Типология рисков *(Risk Typology)*

Для каждого риска определена типология, оценивающая, влияние риска на GxP или на бизнес (соответственно значения «G» и «B» во вложении 1). Риски, связанные с влиянием на бизнес, будут перечислены, но не будут проанализированы, поскольку они не влияют на качество продукта / процесса.  
(For each risk, the Risk Typology has been determined, evaluating if the risk has a GxP or Business impact (respectively G and B values in Attachment 1). Business impact risks will be listed but not further analyzed since they have no impact on the quality of the product/process.)

* + 1. Причины возникновения риска *(Risk Root Cause)*

Причинами возникновения риска могут быть:  
(The Risk Root Cause could be:)

• Неправильная конфигурация-настройки системы (Wrong Configuration)

• Сбой системы (System Failure)

• Человеческий фактор (Human Error)

• Недостаточность функциональных возможностей системы (Lack of system functionality)

• Отсутствие СОП (Lack of SOP)

* + 1. Влияние сбоев (степень воздействия) *(Impacts of Failures (Severity))*

После определения вида сбоя и его последствия, следующим шагом была оценка каждого возможного варианта риска, его влияния (степени воздействия) на качество продукта / процесса.  
(After the failure modes and effects identification, the next step has been the evaluation, for each risk scenario, of the Impact (Severity) on the quality of the product/process.)

Степень воздействия оценивалась в соответствии с критериями, приведёнными в Табл (Table) 1  
(The Severity has been evaluated according to the criteria reported in Табл (Table) 1.)

| **Степень воздействия** *(Severity)* | Критерии для оценки *(Criteria for Evaluation)* |
| --- | --- |
| **Высокая**  ***(High)*** | Бизнес-процесс или функция используются для создания, обновления или обработки данных, которые могут иметь прямое влияние на: *(The business process or function is used to create, update, or process data which may have direct impact upon either:)*   * Эффективность продукта (т.е. кол-во активного ингредиента, эффективность ингредиентов и т.д.) *(Product efficiency (i.e. quantity of active ingredient, potency of ingredients etc.)* * Целостность продукта (загрязнение, перекрёстное загрязнение, хранение и обращение и т.д.) *(Product integrity (contamination, cross contamination, storage and handling etc.)* * Чистота продукта (рецепт, использование ингредиентов) *(Product Purity (i.e. recipe, use of ingredients))* * Целостность данных (т.е. данные, используемые для поддержки регуляторного процесса или их представления) *(Data integrity (i.e. data used to support a regulatory process or submission)* |
| **Средняя**  ***(Medium)*** | Бизнес-процесс или функция используются для создания, обновления или обработки данных, которые оказывают непосредственное влияние на атрибуты качества фармацевтической продукции, в том числе: *(The business process or function is used to create, update or process data, which have direct impact upon pharmaceutical quality attributes including:)*   * Прослеживаемость (т.е. маршрутизация продукта, хранение, перемещение материалов и т.д.) *(Traceability (i.e. product routing, storage, materials movement, etc.))* * Статус (т.е. карантин, выпуск, результаты качества и т.д.) *(Status (i.e. quarantine, release, quality results etc.))* * Количество (т.е. хранение, варианты упаковки и т.д.) *Quantity (i.e. storage, packaging options etc.)* |
| **Низкая**  ***(Low)*** | Бизнес-процесс или функция, используемые для создания, обновления или обработки данных, которые могут оказывать косвенное влияние на атрибуты качества фармацевтического продукта или оказывать прямое влияние на функции, поддерживающие cGxP-операции, такие как: *(The business process or function used to create, update or process data which may have indirect impact upon pharmaceutical quality attributes or a direct impact on those functions that support cGxP operations such as:)*   * Записи об обучении *(Training records)* * Обслуживание параметров безопасности системы или профилей пользователей *(Maintenance of system security settings or user profiles))* * Управление изменениями *(Change Control)* |

Табл (Table) 1 Эффект степени воздействия *(Severity of Effects)*

* + 1. Возможность сбоев (вероятность) *(Probability of Failure (Likelihood))*

Возможность сбоев (вероятность) зависит от уровня настройки / кастомизации системы, например, изменение программного кода. Соответственно, использование только стандартного функционала системы снижает вероятность сбоев системы. Возможность сбоев оценивалась, как указано в Табл (Table) 2.

*(The Probability of Failure (Likelihood) depends on the level of setup / customization of the system, for example, changing the program code. Accordingly, using only the standard system functionality reduces the likelihood of system failures. Probability of Failure was assessed as indicated in Табл (Table) 2.)*

| **Вероятность возникновения** *(Likelihood of occurrence)* | **Коэффициент сбоев** *(Failure Rates)* |
| --- | --- |
| **Высокая**  ***(High)*** | Стандартная системная функция или бизнес-процесс, которые были настроены путём индивидуального кодирования или путём настройки нестандартных системных параметров и / или операций(программирование) *(A standard system function or business process that has been customized by custom coding or by configuration of non-standard system parameters and/or options (programming))* |
| **Средняя**  ***(Medium)*** | Стандартная системная функция или бизнес-процесс, которые были существенно изменены исключительно путём настройки стандартных параметров системы и / или операций *(A standard system function or business process that has been significantly modified solely by configuration of standard system parameters and/or options))* |
| **Низкая**  ***(Low)*** | Стандартная системная функция или бизнес-процесс, которые не были существенно изменены посредством конфигурации или кодирования *(A standard system feature or business process that has not been significantly modified by configuration or coding)* |

Табл *(Table)* 2 Вероятность сбоев *(Likelihood of Failure)*

* + 1. Классы рисков *(Risk Class)*

Класс риска для каждого сценария рисков оценивался как сочетание «степени воздействия» (Табл (Table) 1) и «вероятности» (Табл (Table) 2), как указано в следующей таблице.  
(The Risk Class for each Risk Scenario identified has been evaluated as a combination of the Severity (Табл (Table) 1) and of the Likelihood (Табл (Table) 2), as reported in the following table.)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **Вероятность** *(Likelihood)* | | |
| **Низкая *(Low)*** | **Средняя *(Medium)*** | **Высокая *(High)*** |
| **Степень воздействия** *(Severity)* | **Высокая *(High)*** | **2** | **1** | **1** |
| **Средняя *(Medium)*** | **3** | **2** | **1** |
| **Низкая *(Low)*** | **3** | **3** | **2** |

Табл *(Table)* 3 Классификация риска *(Risk Class)*

Где: (Where:)

• 1 = Высокий (High)

• 2 = Средний (Medium)

• 3 = Низкий (Low)

* + 1. Способность обнаруживать сбои (обнаруживаемость) *(Ability to Detect Failures (Detectability))*

Целью данного этапа является определение, потенциального риска, который может быть распознан и обнаружен (обнаруживаемость) с помощью других средств управления системой. Обнаруживаемость риска оценивалась, как указано в Табл (Table) 4.  
(The purpose of this phase has been to identify if the risk event could be recognized or detected (Detectability) by other system controls. The Detectability of a risk has been evaluated as reported in the Табл (Table) 4.)

|  |  |
| --- | --- |
| **Обнаружение** *(Detection)* | **Критерии для оценки** *(Criteria for Evaluation)* |
| **Низкое**  ***(Low)*** | Независимо от системы, отсутствует автоматическая последующая проверка образцов, или отсутствует процедура (СОП) ручной проверки образцов. *(Independently of the system, there is no downstream automatic samples check, or no formal procedure (SOP) for manual check of the operations.)*  Или *(Or)*  Результаты функции системы не проверяются стандартной проверкой ошибок в системе. *(Any errors in the output of the system function are not checked by a standard system error check)* |
| **Среднее**  ***(Medium)*** | Независимо от системы, есть одна автоматическая последующая проверка образцов или, как минимум, одна процедура ручной проверки процесса. *(Independently of the system, there is one a downstream automatic sample check, or at least one procedure for manual check of the process.)*  Или *(Or)*  Любые ошибки функционала будут проверяться стандартной системной проверкой ошибок (т.е. целостности данных, формата данных, диапазона данных) до завершения действий или процесса или на входе в последующую функцию системы. *(Any errors in the output of the function will be checked by a standard system error check (i.e. integrity of data, format of data, data range) prior to completion of the function or process, or at the input to a subsequent function of the system)* |
| **Высокое**  ***(High)*** | Независимо от системы, продукт проверяется автоматически на 100%, или есть, как минимум, две автоматические проверки последующих образцов. *(Independently of the system, the product is 100% checked automatically, or there are at least two downstream automatic sample checks.)*  И *(and)*  Любые ошибки функционала будут проверяться стандартной системной проверкой ошибок (т.е. целостности данных, формата данных, диапазона данных) до завершения действий или процесса или на входе в последующую функцию системы. *(Any errors in the output of the function will be checked by a standard system error check (i.e. integrity of data, format of data, data range) prior to completion of the function or process, or at the input to a subsequent function of the system)* |

Табл *(Table)* 4 Обнаруживаемость сбоя *(Detectability of Failure)*

* + 1. Оценка приоритета риска *(Risk Priority Evaluation)*

Объединив класс риска и его обнаруживаемость, можно определить степень приоритетности сбоя, связанного с каждым возможным вариантом риска, на основе наибольшей уязвимости.  
(By combining the Risk Class with the Detectability, it is possible to prioritize the fault conditions associated with each risk scenario based upon those areas of greatest vulnerability.)

Приведённая ниже матрица (Табл (Table) 5) представляет модель оценки приоритета риска.  
(The matrix below (Табл (Table) 5) provides the model to evaluate the Risk Priority.)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **Обнаруживаемость** *(Detectability)* | | |
| **Низкая *(Low)*** | **Средняя *(Medium)*** | **Высокая *(High)*** |
| **Класс риска** *(Risk Class)* | 1 | **Высокий *(High)*** | **Высокий *(High)*** | **Средний *(Medium)*** |
| 2 | **Высокий *(High)*** | **Средний *(Medium)*** | **Низкий *(Low)*** |
| 3 | **Средний *(Medium)*** | **Низкий *(Low)*** | **Низкий *(Low)*** |

Табл *(Table)* 5 Приоритетность риска *(Risk Priority)*

* 1. РЕКОМЕНДАЦИИ ДЛЯ ДЕЙСТВИЙ ПО СМЯГЧЕНИЮ РИСКОВ *(GUIDELINES FOR RISK MITIGATION ACTIONS)*

На основе приоритетности для всех возможных рисков, были определены соответствующие меры по снижению риска (например, тестирование, выпуск СОП, внедрение автоматизированного операционного контроля), в соответствии со следующей таблицей:  
(Based on the risk priorities of each Scenario, appropriate Mitigation Actions have been determined (e.g. Testing effort, SOPs emission, automated operational check’s implementation) in order to mitigate the risk, according to the following table:)

|  |  |
| --- | --- |
| **Приоритетность риска** *(Risk Priority)* | **Действия по смягчению последствий** *(Mitigation Action)* |
| **Низкая**  ***(Low)*** | Обучение персонала *(User Training)*  Наличие соответствующих СОП *(Relevant SOPs)* |
| **Средняя**  ***(Medium)*** | Обучение персонала *(User Training)*  Наличие соответствующих СОП *(Relevant SOPs)*  Тестирование в нормальных условиях *(Testing activities in normal conditions)* |
| **Высокая**  ***(High)*** | Обучение персонала *(User Training)*  Наличие соответствующих СОП *(Relevant SOPs)*  Тестирование в нормальных условиях *(Testing activities in normal conditions)*  Усиленное тестирование, где это применимо (например, негативный тест), а также, реализация / верификация процедуры *(Challenge Testing activities where applicable (e.g. negative test) or Procedure Implementation/Verification)* |

Табл *(Table)* 6 Действия по смягчению риска *(Risk Mitigation Actions)*

1. ВЛОЖЕНИЯ *(ATTACHMENTS)*

Вложение 1: Результаты анализа рисков (Attachment 1: Risk Analysis Results)