**ПРИЛОЖЕНИЕ 1**

**Дата: …апреля 2019 г…………………**

**Меморандум о планировании задания**

**Аудиторское задание: ...Аудит информационных технологий.............................................**

# Цель и обоснование задания

*Внедрение нового программного обеспечения SAP HR ERP в Министерстве экономики должно быть завершено к 1 июля 2019 года. За последние годы ряд мелких и крупных ИТ-проектов в нашем госсекторе провалились либо столкнулись с непредвиденными проблемами (финансовыми, операционными и организационными). Генеральный секретарь министерства желает предотвратить такие провалы в будущем. Поэтому новая система SAP будет внедрена только при разумной степени уверенности того, что система обеспечит ожидаемые результаты, и что потенциальные недостатки и риски будут смягчены оптимальным образом. Генеральный секретарь обратился в аудиторский отдел с просьбой предоставить дополнительные гарантии по этим аспектам, а также по процессу управления реализацией самого проекта.*

# Описание деятельности организации и аудируемого процесса

## Аудируемый процесс

*Система SAP-HR внедряется посредством организации временного проекта, отвечающего за бесперебойное осуществление. Новая система SAP-HR интегрирует следующие процессы: расчет заработной платы, администрирование персонала, управление рабочим временем, управление командировками, формирование отчетности.*

*Команда проекта состоит из руководителя проекта, сотрудников информационного управления и внешнего консультанта по SAP. Начальник информационного управления (CIO) несет общую ответственность за проект. Согласно плану, проект разработан на основе руководящих принципов Prince-2 (Projects in Control 2).*

*Реализация проекта предусматривает следующие этапы:*

1. *Оценка текущей ситуации;*
2. *План управления изменениями (+ план обеспечения непрерывности деятельности);*
3. *Проведение этапа тестирования;*
4. *Момент перехода: запуск 1 июля.*

*Ключевые цели, сопряженные с переходом на новую систему:*

*•• Улучшить работу отдела кадров;*

*•• Более эффективно принимать более рациональные решения (управленческая цель);*

*•• Улучшить прохождение информации между разными отделами;*

*•• Модернизировать ИТ-платформу для кадровых процессов;*

*•• Единая точка входа и информации по всем кадровым вопросам;*

*•• Ликвидация ручных операций, меньше ошибок;*

*•• Лучше интегрированные процессы и прозрачность;*

*•• Повышение производительности и эффективности;*

*•• Сокращение эксплуатационных затрат благодаря ликвидации устаревших систем.*

# Основные риски, связанные с аудируемыми процессами

*Типичные риски, связанные с внедрением похожих систем (и перезодом на них), обычно определяются при помощи триады КЦД:* ***К****онфиденциальность (риск потери/утечки критически важной или конфиденциальной информации третьим лицам),* ***Ц****елостность (надежность данных, выдаваемых системой) и* ***Д****оступность (непрерывность, резервные копии, восстановление данных и проч.). Вообще, чтобы эффективно работать с рисками, связанными с триадой КЦД, необходима достаточное сочетание прикладных и общетехнологических средств контроля.*

*Прочие риски связаны с поэтапным подходом, предусмотренным в структуре проекта, который должен обеспечить успешное внедрение новой системы: риски, связанные с надлежащей организацией управления самого ИТ-проекта.*

# Цели и объем аудиторского задания:

*Целью аудита является предоставить разумную гарантию по следующим ключевым аудиторским вопросам:*

* *Организовано и функционирует ли* ***управление*** *проектом таким образом, чтобы обеспечить успешную миграцию и внедрение SAP-HR в Министерстве экономики?*
* ***Достаточно ли адекватны*** *прикладные и общетехнологические средства контроля с точки зрения конфиденциальности, целостности данных и доступности критически важной информации из связанных с кадрами систем на этапе проектирования, миграции и осуществления проекта?*

## *Заключения о подтверждении надлежащего управления проектом, а также адекватности контроля КЦД на прикладном и общетехнологическом уровне сопровождаются рекомендациями, где это необходимо и применимо. Потенциальные заключения и рекомендации.*

*Критерии аудита берутся из следующей справочной базы аудитора:*

* ***Prince2:*** *за основу в оценке надлежащего управления проектом берутся следующие принципы Prince2: бизнес-кейс (непрерывное бизнес-обоснование), определенные роли и обязанности по структуре Prince2, управление по стадиям (поэтапный подход, включая управление рисками) и акцент на продуктах согласно предварительно определенным уровням толерантности к риску. Весь набор норм касательно данных принципов описан в приложении;*
* ***COBIT5:*** *Критерии триады КЦД происходят из следующих модулей COBIT-5: Координация/планирование/организация (APO), Разработка/приобретение/внедрение (BAI), Предоставление/обслуживание/поддержка (DSS) и*

*Мониторинг/оценка/анализ (MEA).*

*Модули COBIT5 описывают критерии по каждому этапу, начиная с планирования до полного внедрения информационных систем в организации любого типа. Критически важные критерии модулей, согласованные с CIO, ложатся в основу заключения о подтверждении адекватности общетехнологических и прикладных средств контроля на каждом этапе реализации;*

* *Существующие организационные* ***Процедуры и правила****,**имеющие отношение к процессу перехода на новую систему SAP-HR. Если данные процедуры и правила противоречат требованиям Prince2 и/или COBIT5, формируется соответствующее заключение аудитора.*

## Объем:

*В ходе аудита не предусмотрено увеличение объёма за счёт оценки ключевых задач, поставленных в рамках перехода на новую систему.*

# Методология аудита

|  |  |  |  |
| --- | --- | --- | --- |
| Цель/вопрос аудита | Ключевые аспекты | Критерии | Методология(инструментарий аудита) |
| **Надлежащее управление:** соответствует ли дизайн и работа проекта принципам Prince-2 на каждом этапе реализации? | Бизнес-обоснование | * БО обновляется на каждом этапе проекта
* Обоснование проекта должно согласовываться со стратегией организации или программы.
* План проекта и БО должны быть согласованы.
* Преимущества должны быть четко определены и обоснованы.
* Должно быть ясно, каким образом будут реализованы преимущества
 |  |
| Роли и обязанности | * Исполнительные функции и управление проектом четко разделены
* и т.д.
 |  |
| **Достаточность общих мер контроля:** хорошо ли контролируются/ организованы ключевые ИТ-процессы в организации? | COBIT/APO12Управление рисками | * Проведена полномасштабная оценка рисков, связанных с миграцией на SAP-HR;
* Посвященный рискам раздел в проектном документе охватывает правильные вопросы
* и т.д.
 |  |
| **Достаточность прикладных мер контроля:** достаточны ли контрольные механизмы, встроенные во внедряемую новую систему (сами по себе и в комплексе с другими системами на этапе миграции), для смягчения рисков, связанных с триадой КЦД? | COBIT/DSS04Управление непрерывностью | * Процедуры сохранения резервных копий и восстановления осуществляются в работающем ПО на этапе миграции
* ПО содержит автоматизированные положения на случай сбоев
 |  |

## Программа аудита

*Данное аудиторское задание проводится параллельно по двум направлениям:*

***Деятельность, связанная с предоставлением разумной гарантии в отношении управления проектом:*** *команда аудиторов проводит аудиторские мероприятия в режиме реального времени, следуя этапам аудируемого проекта. Каждый этап проекта (4 этапа) требует одобрения команды аудиторов перед тем, как может быть начато осуществление следующего этапа. Команда аудиторов непрерывно отслеживает и оценивает соблюдение принципов Prince2. Все документы, формируемые проектом, могут использоваться в качестве свидетельств аудита. Время от времени проводятся интервью с членами команды проекта, руководством (CIO) и другими имеющими отношение к процессу сторонами (например, кадровый отдел, информационное управление);*

***Деятельность, связанная с предоставлением разумной гарантии в отношении достаточности общетехнологических и прикладных средств контроля:*** *в отношении как общетехнологических, так и прикладных средств контроля применяется широкая гамма методов аудита. Например, различные виды тестирования (на прикладном уровне - на предмет вторжения, на безопасность, надежность, целостность). Также проводятся интервью с представителями информационного отдела, кадровых отделов, отделов формирования политики, руководства (в т.ч. CIO). Основой для формирования нашего заключения служат принципы и базовые критерии COBIT5.*

*Обе команды аудиторов регулярно встречаются, чтобы обмениваться информацией друг с другом. Оба направления деятельности считаются одним аудиторским заданием.*

**Основные этапы аудита:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 1 этап проекта(январь 2019 г.) | 2 этап проекта(июль 2019 г.) | 3 этап проекта(декабрь 2019 г.) | 4 этап проекта (июль 2020 г.) |
| **Аудит проекта:**400 часов x 2 команды аудиторов: 800 часов | В реальном времени + продолжать/не продолжать после этапа + промежуточный отчет | В реальном времени + продолжать/не продолжать после этапа + промежуточный отчет | В реальном времени + продолжать/не продолжать после этапа + промежуточный отчет | В реальном времени + продолжать/не продолжать после этапа + промежуточный отчет в сочетании с заключением аудитора касательно средств контроля |
| **Аудит общих и информационных мер контроля**300 часов x 2 команды аудиторов: 600 часов | Предварительное изучение | Предварительный/ промежуточный отчет о проектных средствах контроля, связанных с планом управления изменениями (APO+BAI) | Предварительный/ промежуточный отчет о работе средств контроля на этапе тестирования(DSS+MEA) | Предварительный/ общий отчет о работе средств контроля на этапе трансформации и внедрения(DSS+MEA) в сочетании с заключением аудитора касательно проекта |

## Ресурсы

*Аудит проводится в соответствии с уставом аудита аудиторского отдела Министерства финансов. Информация, требующая конфиденциальности, используется согласно положениям данного устава.*

|  |  |  |
| --- | --- | --- |
| **Роль** | **Имя** | **Должность** |
| Руководитель проекта | Опытный оценщик/аудитор ERP (планирования корпоративных ресурсов) |  |
| Один аудитор эффективности | Сертифицированный по методике Prince2 |  |
| Два сертифицированных ИТ-аудитора | Опыт в оценках с применением COBIT |  |

# Потенциальные трудности (если применимо)

*Риск для аудита заключается в том, что проект будет отложен в связи с непредвиденными обстоятельствами. В таком случае, проведение аудита замораживается, и специалисты занимаются другими заданиями, пока проект не возобновится.*