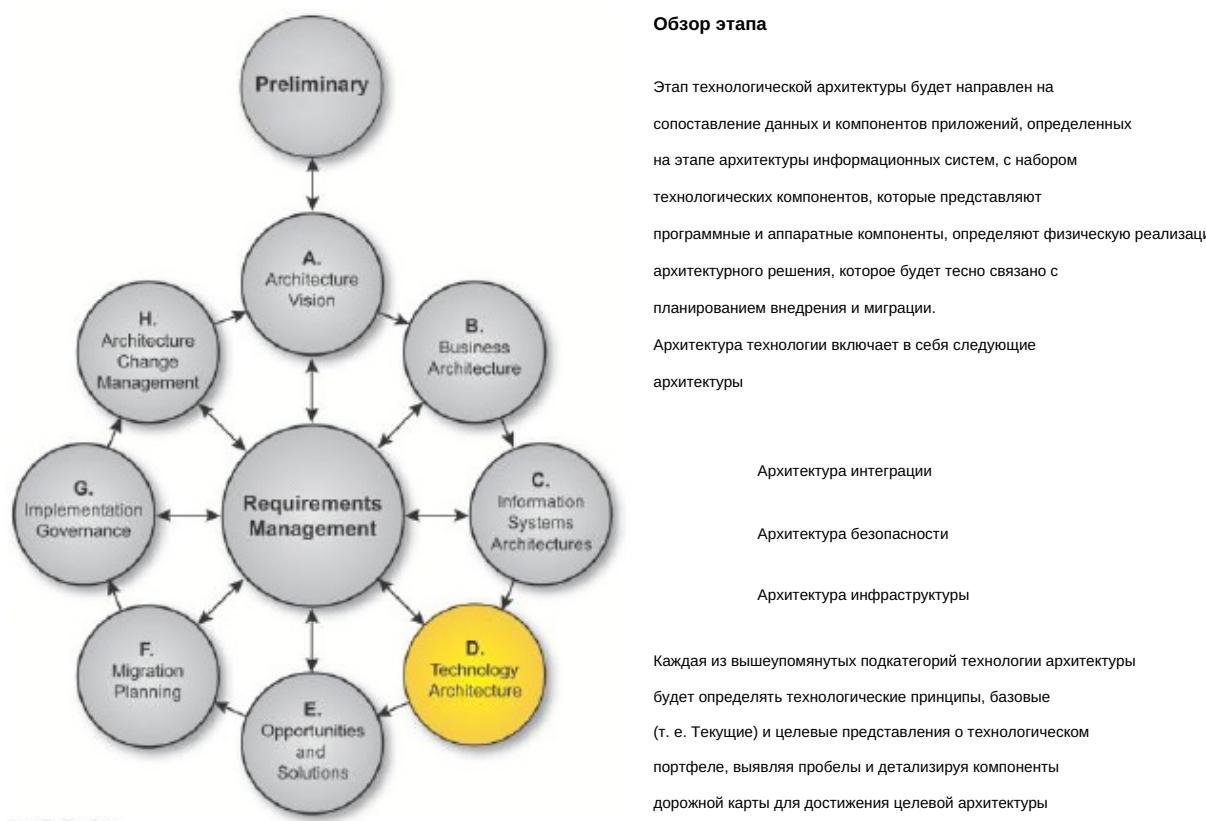


## **7. Фаза D TOGAF ADM -**

### ***Архитектура технологии***

## 7. Этап D: Технология

### Архитектура



#### 7.1 Принципы технологической архитектуры

##### Принципы технологической архитектуры (Включая интеграцию, инфраструктуру и безопасность)

- Функциональная совместимость
- Конфиденциальность
- Основанные на открытых стандартах
- Национальный шлюз предоставления услуг на базе ESB
- Веб-сервисы для обмена информацией и детализированного обслуживания. Масштабируемость, доступность, резервное копирование и архивирование
- Контроль безопасности
- Соответствие требованиям, Выбор и стандартизация Уровней безопасности
- Измерение безопасности
- Использование общей системы аутентификации пользователей

## 7.2 Архитектура интеграции

### 7.2.1 Принципы архитектуры интеграции

Принцип № 1	
Имя	Функциональная совместимость
Заявление	<p>Определенная политика должна усиливать, а выбранные стандарты должны способствовать интероперабельности</p> <p>Определите общие компоненты (включая существующую государственную политику, стандарты, применение, технологии и т.д. везде, где это уместно) во всей области функциональной совместимости и определяют политики, стандарты и процедуры для обеспечения возможности повторного использования артефактов. Например, для определения структуры данных, наборов данных на национальном уровне и т.д. Выберите стандарты, которые обеспечивают больший выбор и снижают административную нагрузку.</p>
Обоснование	<p>Устраняет разнородность ИКТ-решений в различных государственных учреждениях, которые не могут "разговаривать" или обмениваться данными. Интероперабельность обеспечивает беспрепятственный обмен информацией, повторное использование моделей данных и взаимозаменяемость данных в разных системах.</p> <p>Обеспечивает возможность эффективного взаимодействия, совместной работы, доступа к данным и облегчения их интеграции для обеспечения связи между различными правительственными организациями (G2G, G2C, G2B и т.д.).</p>

Принцип № 2	
Имя	Конфиденциальность
Заявление	Гарантирует конфиденциальность информации в отношении граждан (например, медицинских карт), бизнеса (например, статистики организаций) и правительства (например, соглашений о конфиденциальности) для обеспечения соблюдения установленных законом ограничений на доступ и распространение информации
Обоснование	Это обеспечит надлежащую классификацию конфиденциальной информации и данных и надлежащую защиту. Конфиденциальность не может быть гарантирована одними техническими стандартами, для ее обеспечения должны существовать процессы, межорганизационные соглашения, законы о кибербезопасности и т.д. Однако фундаментальным принципом этого является защита целостности правительской информации и информации, находящейся в распоряжении различных агентств.

Принцип № 3	
Имя	Основанные на открытых стандартах
Заявление	Следует поощрять соблюдение открытых стандартов
Обоснование	Приверженность стандарту, который обеспечит выбор поставщика, будет способствовать конкурентоспособности и возможности взглянуть на кроссплатформенность. Атрибуты открытых стандартов, такие как независимость от платформы, нейтральность поставщика и возможность использования в нескольких реализациях, а также модель установления открытых стандартов - это то, что обеспечит устойчивый обмен информацией, интероперабельность, гибкость, сохранение данных и большую свободу от технологий и привязки к поставщику.

Принятие открытых стандартов облегчит хранение электронных национальных записей и данных с использованием открытых форматов файлов данных.

#### Принцип № 4

<b>Имя</b>	Национальный шлюз предоставления услуг на базе ESB
<b>Заявление</b>	<p>Корпоративная служебная шина (ESB) должна быть общедоступным API для базовой реализации Шлюза предоставления услуг в масштабах предприятия. В результате он должен быть доступен в качестве ресурса для любых сервисных компонентов на предприятии.</p> <p>Между сервисом и нижележащими за ним слоями должна быть слабая связь, при этом уровень сервиса действует как фасад слоя под ним. Клиенты Шлюза предоставления услуг не должны иметь представления о различных сервисных доменах, расположенных под ним.</p>
<b>Обоснование</b>	<p>Использование ESB способствует ослаблению связи, поддерживает интеграцию разнородных систем, поддерживает соблюдение открытых стандартов</p> <p>ESB обеспечивает быструю разработку, сборку и внедрение сервисов, простоту обслуживания и улучшенную видимость бизнеса.</p>

#### Принцип № 5

<b>Имя</b>	Веб-сервисы для обмена информацией и детализированного обслуживания.
<b>Заявление</b>	<p>Веб-сервисы должны использоваться между уровнями обслуживания. Степень детализации сервисов, входящих в ESB, не должна быть слишком высокой для продвижения огромного количества неуправляемых сервисов, где изменение в одном приводит к каскадному набору изменений с согласованными другими</p>
<b>Обоснование</b>	<p>Используя веб-службы для взаимодействия между уровнями обслуживания, предприятие может создать возможность иметь рационализированную стратегию мониторинга и безопасности для предприятия, обеспечивающую соответствие OASIS WS-* отраслевым стандартным спецификациям веб-служб безопасности, интероперабельности, надежности и т. д.</p>
<b>Последствия</b>	<p>Руководящему комитету, работающему над моделями консенсуса, наивысших общих факторов и основанными на анализе фреймворками, следует принять решение о полезной нагрузке запросов и ответов составленных сервисов</p>

#### 7.2.2 Базовая архитектура интеграции

На итерации 1 цикла ADM интеграция между приложениями отсутствует.

#### 7.2.3 Целевая архитектура интеграции

### Обзор шлюза предоставления услуг GEA в Непале.

Для реализации концепции электронного правительства "Создание сети ценностей в Непале", чтобы сделать все государственные услуги доступными для простых граждан и обеспечить эффективность, прозрачность и надежность таких услуг, крайне важна необходимость сотрудничества, совместной работы и интеграции информации между различными правительственными ведомствами.

В рамках консолидации и интеграции государственных услуг между министерствами / департаментами был концептуализирован общий шлюз для предоставления интегрированных услуг. Был определен и спроектирован предлагаемый шлюз предоставления услуг GEA в Непале (NGSDG), который будет действовать как открытая стандартная корпоративная сервисная шина и обеспечивать бесперебойную интероперабельность и обмен данными и событиями между подразделениями.

Основные моменты NGSDG кратко изложены ниже -

NGSDG обеспечит поддержку сервис-ориентированной архитектуры (SOA) и будет действовать как корпоративная сервисная шина для всех взаимодействий между потребителями услуг (гражданами и предприятиями) и различными поставщиками услуг (правительственными ведомствами) и даже между правительственными ведомствами. Поддержка обслуживания устаревших приложений - С помощью NGSDG устаревшие приложения могут предлагать свои услуги различным другим потребителям, подключенным к корпоративной сервиснойшине.

Способен обрабатывать большое количество транзакций по всей сети, обеспечивает общий набор спецификаций и единой точки доступа.

Безопасность и аудит - Обеспечивает лучшее отслеживание (аудит) и безопасность каждого вызова службы и обеспечивает государственный контроль с помощью полных журналов аудита и временной отметки транзакций

Функциональная совместимость - корпоративная служебная шина SDG в качестве промежуточного программного обеспечения обеспечивает бесперебойную работу

функциональная совместимость и облегчит простой обмен данными и событиями между подразделениями.

Обеспечьте преобразование данных и форматов, если таковые имеются, наряду с маршрутизацией и фильтрацией данных.

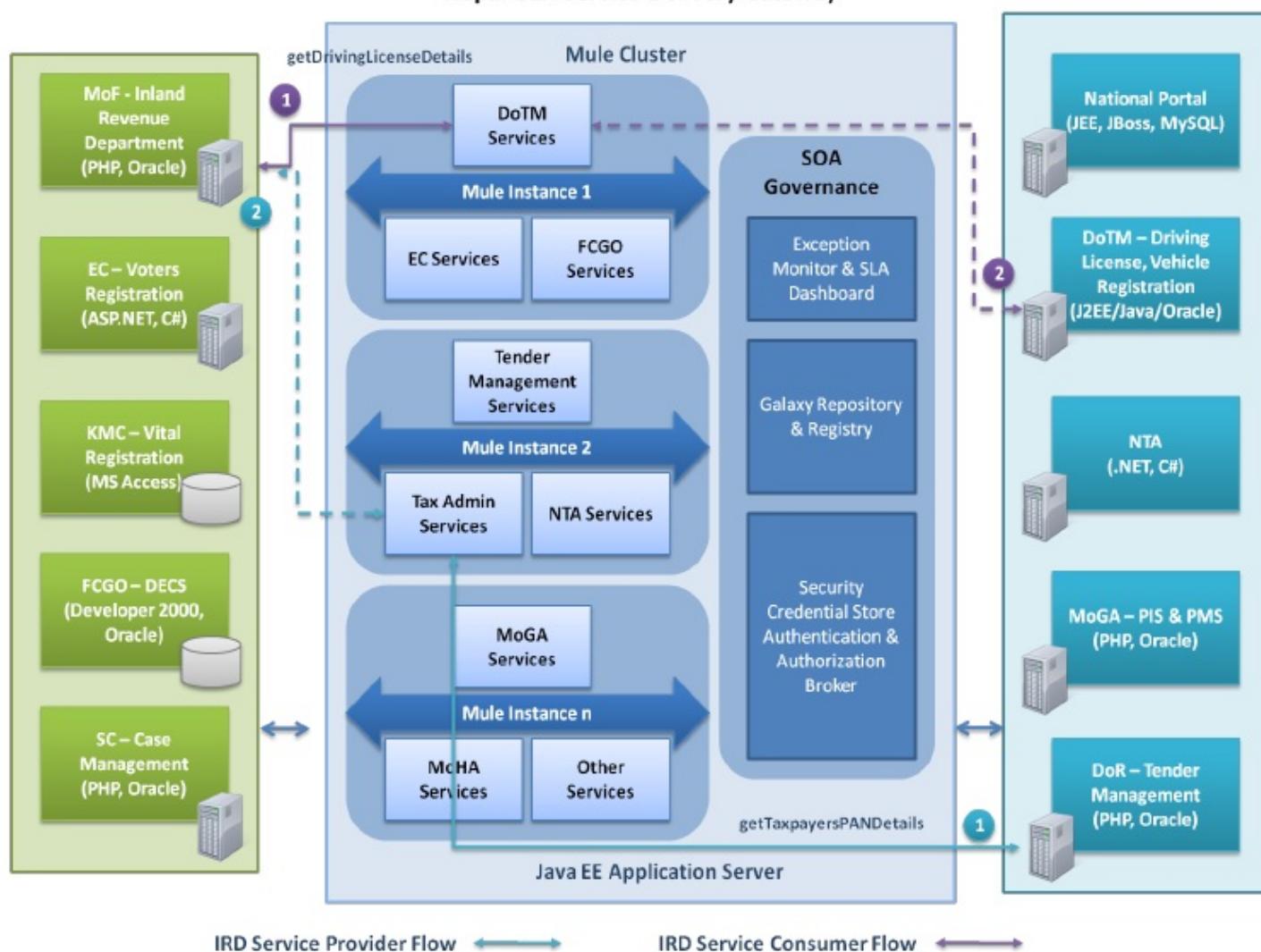
Облегчать синхронизацию и координацию межведомственной работы в режиме реального времени и почти в режиме реального времени, отслеживая все транзакции правительства Непала. Общие сервисы - В будущем SDG Enterprise Service Bus сможет добавлять дополнительные функциональные возможности для поддержки общих сервисов, таких как аутентификация, интерфейс платежного шлюза, службы коротких сообщений, службы мгновенных сообщений и т.д. Предоставляет необходимые соединители для взаимодействия с приложениями, разработанными на уровне отдела.

Разработка и внедрение шлюза предоставления услуг GEA для правительства Непала основаны на продукте ESB с открытым исходным кодом на основе открытого стандарта -Mule!!

### Топология ESB

Шлюз доставки услуг Nepal Government Enterprise Architecture, основанный на Mule, задуман как облегченная платформа обмена сообщениями и высокораспространяемый объектный брокер. В следующей топологии для Service шлюза доставки службы Mule действуют как посредники для приложений-потребителей услуг, заботясь о вызове удаленных служб для приложений-поставщиков услуг. Все знания удаленной службы сосредоточены в одном месте - кластерах экземпляров Mule, которые действуют как прокси. Эти знания включают в себя не только сведения о подключении, но также могут охватывать конфигурации безопасности, конкретные преобразования данных, специфическую маршрутизацию и фильтрацию на основе контента и организацию обслуживания.

## Nepal GEA Service Delivery Gateway

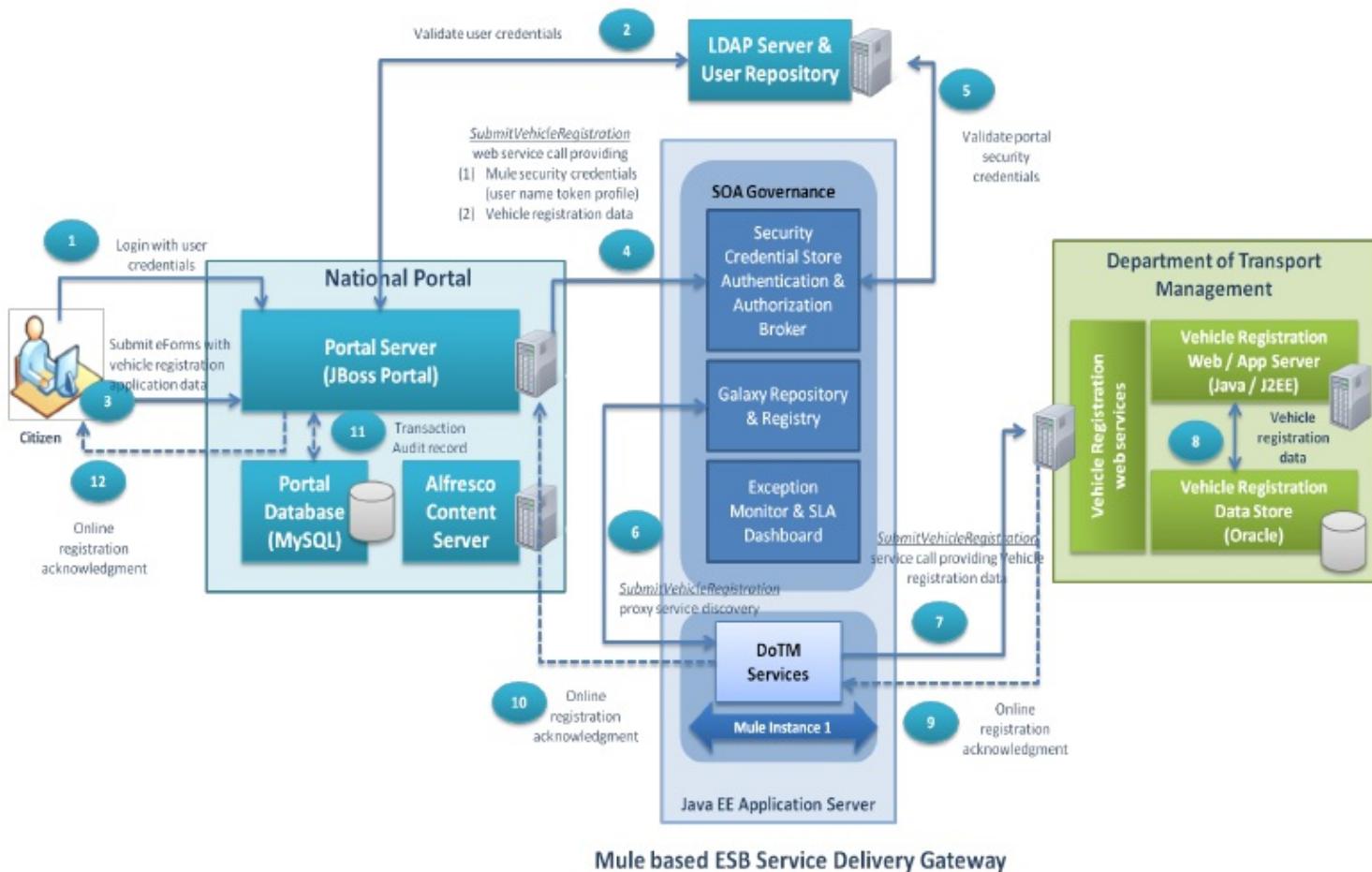


В приведенной выше топологии несколько экземпляров Mule будут развернуты в кластере экземпляров Mule для размещения на сервере приложений JEE . В каждом экземпляре Mule будет развернут свой набор государственных услуг. Точное количество государственных услуг, которые будут развернуты в каждом экземпляре, будет окончательно определено на этапе внедрения. Однако службы, которые будут развернуты в каждом экземпляре Mule, могут быть классифицированы в зависимости от отделов или типа услуг, например, для граждан, предприятий, служащих и т.д.

Чтобы проиллюстрировать обмен информацией через NGSDG, были изображены некоторые сценарии сквозного использования ниже, чтобы продемонстрировать, как вышеупомянутая топология ESB может быть использована в качестве интеграционной платформы для обмена информацией между подразделениями.

**Сценарий использования 1: Процесс онлайн-регистрации транспортного средства**

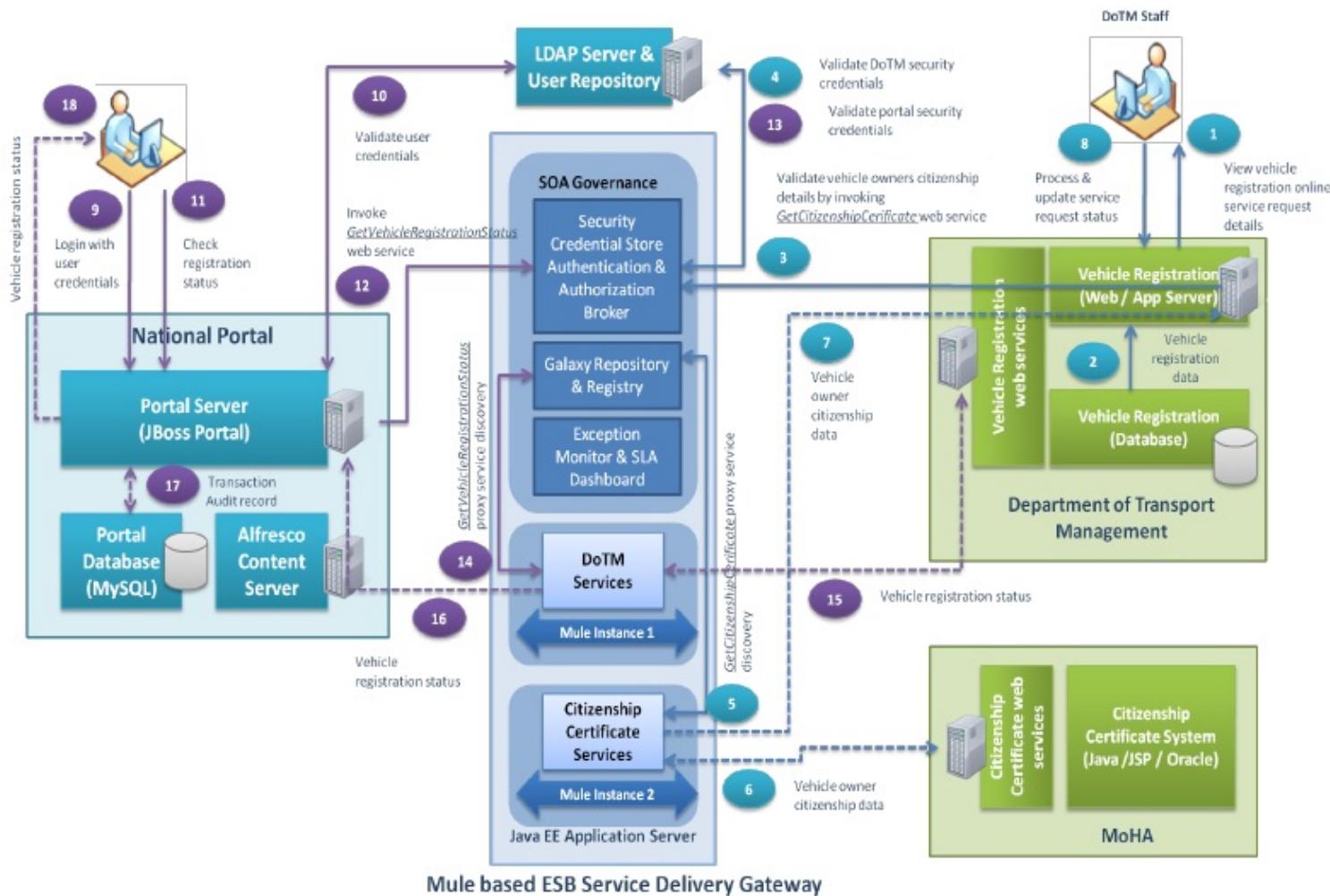
1: Гражданин отправляет онлайн-запрос на регистрацию транспортного средства с национального портала



Шаг	Описание шага
1.	Гражданин входит в систему Национального портала с учетными данными пользователя. Гражданину потребуется зарегистрироваться онлайн на национальном портале, прежде чем входить в систему с помощью опции "Регистрация пользователя". Онлайн-учетные данные пользователя, предоставленные в рамках процесса регистрации Пользователя, потребуются гражданину для входа на национальный портал.
2.	Национальный портал проверяет подлинность учетных данных пользователя в пользовательском репозитории в LDAP. Если проверка подлинности завершается неудачей, портал возвращает сообщение об ошибке. Если аутентификация прошла успешно, пользователю разрешается войти на национальный портал, чтобы воспользоваться государственной электронной услугой.
3.	Пользователь выбирает службу управления транспортом "Регистрация транспортных средств" и выбирает онлайн-заявку на регистрацию транспортного средства. Пользователю будет представлена онлайн-форма регистрации транспортного средства. Пользователь заполняет онлайн-форму с соответствующей требуемой информацией и отправляет онлайн-форму.

Шаг	Описание шага
НЕТ	
4.	<p>После отправки портал преобразует собранные данные онлайн-формы в формат xml-сообщения который отправляется прослушивающему серверу, запущенному на сервере портала. Сервлет обработает запрос и, в свою очередь, выполнит метод приложения "SubmitVehicleRegistration" для определенного пользователя. Прокси-сервера портала будут добавлены в качестве заголовка сообщения. Данные формы и учетные данные пользователя citizen будут переданы в качестве запросов на ввод веб-службой и будут частью тела сообщения. Экземпляр портала, развернутый в GIDC, попытается установить соединение с центральным Mule инфраструктурой ESB на основе соответствующих учетных данных безопасности аутентификации для вызова веб-службы SubmitVehicleRegistration  </p>
5.	<p>Mule проверяет подлинность идентификатора пользователя и пароля, указанных в профиле токена имени пользователя, переданном экземпляром портала в репозитории пользователей LDAP. Если профиль токена имени пользователя недействителен, Mule выполнит ожидание и вернет сообщение об ошибке сообщение возвращается обратно на портал. Если маркер имени пользователя действителен, Mule проверит, авторизован ли профиль пользователя соответствующий веб-сервис. Если профиль пользователя не авторизован для доступа к веб-службе, Mule вернет порталу сообщение об ошибке. Если профиль токена имени пользователя действителен и авторизован для доступа к веб-службе, Mule продолжит дальнейшую обработку запроса, как указано в шаге 6</p> <p>Mule -DoTM Services  , который действует как прокси для базовой веб-службы</p>
6.	<p>-SubmitVehicleRegistration  , развернутый на сервере DoTM, будет развернут в экземпляре Mule 1. Этот прокси-сервис будет зарегистрирован в реестре Galaxy. Mule вызовет "Службы DoTM", развернутые в экземпляре Mule 1, посредством обнаружения службой уже зарегистрированной службы "SubmitVehicleRegistration" в реестре Galaxy. Mule proxy -Служба DoTM   установит соединение с DoTM web для конкретного подразделения сервера, на котором размещена система регистрации транспортных средств и веб-служба</p>
7.	<p>SubmitVehicleRegistration Будет вызвана веб-служба SubmitVehicleRegistration, размещенная на сервере DoTM. Онлайн запрос, инициированный с национального портала, поступит на сервер департамента через шлюз доставки услуг ESB на основе Mule Веб-служба DoTM SubmitVehicleRegistration обработает</p>
8.	<p>данные формы, предоставленные гражданином, и сохранит их в хранилище данных.</p>
9.	<p>Подтверждение онлайн-заявки с контрольным номером / application number будет возвращено как часть обратного ответа Mule -Службе DoTM  </p>
10.	<p>Служба Mule DoTM, развернутая в экземпляре Mule 1, вернет ответ, предоставленный службой DoTM, обратно на сервер портала</p>
11.	<p>Детали аудита транзакций сохраняются в хранилище данных портала Портал отображает ответ онлайн гражданину, предоставляющему контрольный номер /</p>
12.	<p>регистрационный номер заявки для отслеживания статуса онлайн-заявки</p>

2: DoTM обрабатывает запрос на обслуживание для регистрации транспортного средства и проверяет  
статус регистрации гражданина с Национального портала



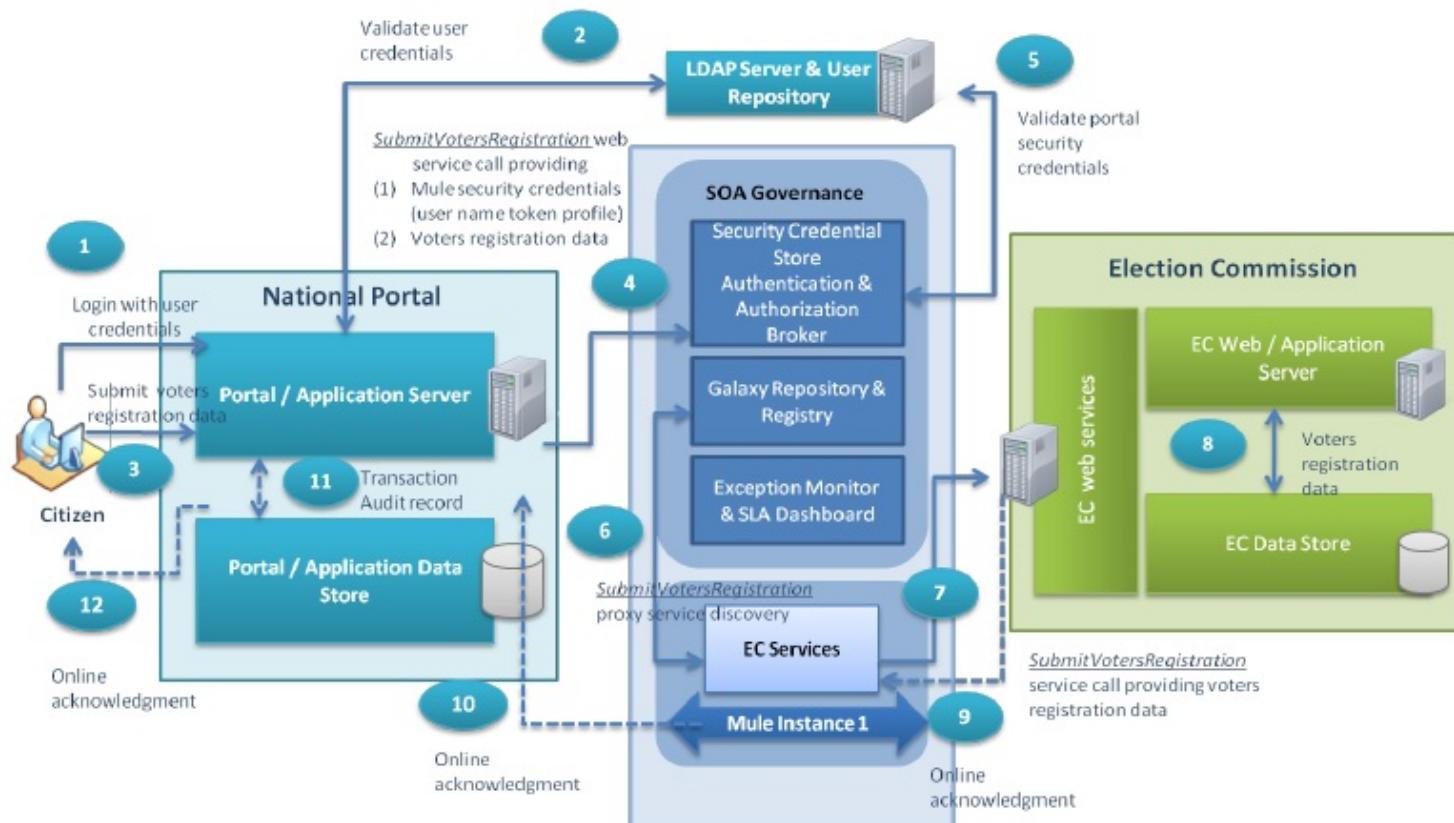
Шаг	Описание шага
1.	Сотрудники департамента DoTM входят в приложение для конкретного департамента, чтобы просмотреть онлайн данные о регистрации транспортного средства, предоставленные гражданином в предыдущем варианте использования
2.	Детали запроса на обслуживание для регистрации транспортного средства для гражданина, зафиксированные на сервере базы данных DoTM , извлекаются и отображаются сотрудникам DoTM.
3.	<p>В рамках проверки данных о гражданстве владельца транспортного средства, предоставленных владельцем транспортного средства,</p> <p><b>Маркер имени пользователя</b> для прокси-сервера DoTM, определенного пользователем, будет добавлен в качестве заголовка сообщения подразделения <b>Имя владельца транспортного средства (предыдущина)</b> и номер гражданства будут переданы в качестве входных данных веб-службы</p> <p>запросы будут частью тела сообщения. Экземпляр приложения DoTM, развернутый на сервере DoTM, попытается установить соединение с центральной инфраструктурой ESB на основе Mule с соответствующими учетными данными безопасности аутентификации (профиль токена имени пользователя ) для вызова веб-службы "GetCitizenshipCertificate"</p>

Шаг	Описание шага
НЕТ	
4.	Mule проверит подлинность идентификатора пользователя и пароля, указанных в переданном профиле токена имени пользователя экземпляром приложения DoTM в репозитории пользователей LDAP. Если профиль токена имени пользователя недействителен, Mule обработает исключение и вернет ошибку отправьте ответное сообщение приложению DoTM. Если маркер имени пользователя действителен, Mule проверит, авторизован ли профиль пользователя соответствующий веб-сервис. Если профиль пользователя не авторизован для доступа к для доступа к веб-службе, Mule вернет сообщение об ошибке обратно в приложение DoTM. Если профиль токена имени пользователя действителен и авторизован для доступа к веб-службе, Mule продолжит дальнейшую обработку запроса
5.	Mule -Службы сертификатов гражданства, которые действуют как прокси для базовой веб-службы -GetCitizenshipCertificate, развернутые на сервере MoHA, будут развернуты в экземпляре Mule 2. Этот прокси-сервис будет зарегистрирован в реестре Galaxy Mule вызовет "Службы сертификатов гражданства", развернутые в экземпляре Mule 2, посредством обнаружения службой уже зарегистрированной службы "GetCitizenshipCertificate" в реестре Galaxy . Mule proxy -службы
6.	получения сертификата гражданства установит соединение с Министерством здравоохранения сервер, относящийся к конкретному ведомству, на котором размещен веб-сервис GetCitizenshipCertificate. Будет вызван веб-сервис GetCitizenshipCertificate, размещенный на сервере MoHA. Онлайн запрос, инициированный приложением DoTM, поступит на сервер департамента министерства здравоохранения через шлюз доставки услуг ESB на основе Mule Веб-служба обработает запрос, получив доступ к хранилищу данных департамента, которое фиксирует сведения о гражданстве. Если найдена соответствующая запись для конкретного имени гражданина и номера гражданства, запись является извлекается и возвращается как часть выходного ответа обратно в Mule -Сертификат гражданства Services. Если соответствующая запись не найдена, веб-служба вернет соответствующее сообщение об ошибке. Служба Mule -Citizenship Certificate Services, развернутая в экземпляре Mule 2, вернет ответ обратно на вызывающий веб-сервер / сервер приложений DoTM Сотрудники DoTM проверят возвращенный ответ и продолжат обработку запроса на регистрацию транспортного средства .
7.	На различных этапах обработки запроса онлайн-сервиса на регистрацию транспортного средства сотрудники DoTM обновят статус заявки.
9.	Владелец транспортного средства, чтобы проверить свой статус онлайн-регистрации транспортного средства, войдет в систему на Национальном портале с учетными данными пользователя. Учетные данные онлайн-пользователя, предоставленные в рамках процесса регистрации пользователя , потребуются гражданину для входа на национальный портал.
10.	Национальный портал проверяет подлинность учетных данных пользователя в пользовательском репозитории в LDAP. Если проверка подлинности завершается неудачей, портал возвращает сообщение об ошибке Если аутентификация прошла успешно, владельцу транспортного средства разрешается войти на национальный портал, чтобы воспользоваться услугами правительства. электронное обслуживание
11.	Пользователь выбирает Департамент управления транспортом -Статус регистрации транспортного средств Популярная опция eService. Пользователь вводит онлайн-регистрационный номер и имя владельца транспортного средства и отправляет запрос

Шаг	Описание шага
НЕТ	
	<p>чтобы проверить текущее состояние онлайн-регистрации, инициированной им в предыдущем варианте использования</p>
12.	<p>После отправки портал преобразует собранные онлайн-данные в формат xml-сообщений, который отправляется прослушивающему серверу, запущенному на сервере портала. Сервлет обработает запрос и, в свою очередь, вызовет "GetVehicleRegistrationStatus" маркер имени пользователя для определенного пользователя прокси-сервера портала будет добавлен в заголовок сообщения. Регистрационный номер и учетные данные гражданина-пользователя будут переданы в качестве входных данных веб-службы, запрашивает и будет частью тела сообщения. Экземпляр портала, развернутый в GIDC, попытается установить соединение с центральным Mule инфраструктурой ESB на основе соответствующих учетных данных безопасности аутентификации для вызова -GetVehicleRegistrationStatus веб-службы</p>
13.	<p>Mule проверяет подлинность идентификатора пользователя и пароля, указанных в профиле токена имени пользователя, переданном экземпляром портала в репозитории пользователей LDAP. Если профиль токена имени пользователя недействителен, Mule выполнит ожидание и вернет сообщение об ошибке, сообщение возвращается обратно на портал. Если маркер имени пользователя действителен, Mule проверит, авторизован ли профиль пользователя соответствующий веб-сервис. Если профиль пользователя не авторизован для доступа к веб-службе, Mule вернет порталу сообщение об ошибке. Если профиль токена имени пользователя действителен и авторизован для доступа к веб-службе, Mule продолжит дальнейшую обработку запроса Служба Mule -DoTMII, которая действует как прокси-сервер для базовой веб-службы, -GetVehicleRegistrationStatus, развернутая на сервере DoTM, будет развернута в экземпляре Mule 1. Эта прокси-служба будет зарегистрирована в реестре Galaxy. Mule вызовет службы -DoTMII, развернутые в экземпляре Mule 1, посредством обнаружения службой уже зарегистрированной службы -GetVehicleRegistrationStatus в реестре Galaxy . Mule proxy -Службы DoTMII установят соединение с сервером, относящимся к конкретному отделу DoTM на котором размещена веб-служба GetVehicleRegistrationStatus</p>
14.	<p>Будет вызвана веб-служба GetVehicleRegistrationStatus, размещенная на сервере DoTM. Онлайн-запрос, инициированный с национального портала, поступит на сервер департамента DoTM через шлюз доставки услуг ESB на основе Mule Веб-служба обработает запрос, получив доступ к хранилищу данных департамента, которое фиксирует регистрационные данные транспортного средства. Если найдена соответствующая запись для имени и регистрационного номера конкретного владельца транспортного средства, то запись извлекается и возвращается как часть выходного ответа обратно в Mule -Службы DoTMII. Если соответствующая запись не найдена, веб-служба вернет</p>
15.	<p>соответствующее сообщение об ошибке. Служба Mule DoTM, развернутая в экземпляре Mule 1, вернет ответ, предоставленный службой DoTM, обратно на сервер портала</p>
16.	<p>Сведения об аудите транзакции сохраняются в хранилище данных портала</p>
17.	<p>Портал отображает ответ гражданину с обновлением статуса, если таковой имеется.</p>

**Сценарий использования 2: Процесс онлайн-регистрации избирателей**

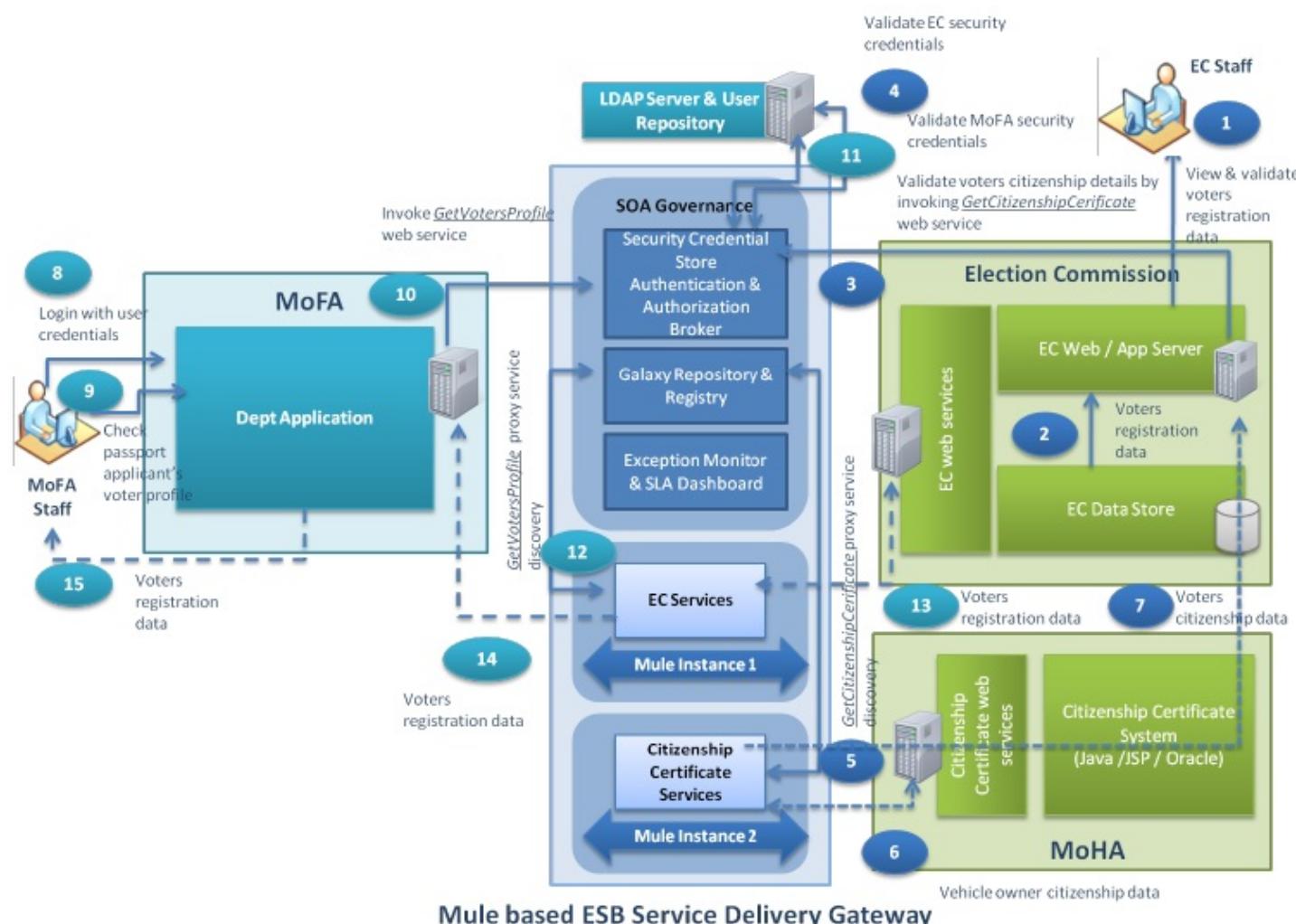
1. Гражданин подает онлайн-запрос на регистрацию избирателя с Национального портала

**Mule based ESB Service Delivery Gateway**

Шаг НЕТ	Описание шага
1.	Гражданин входит в систему Национального портала с учетными данными пользователя. Гражданину потребуется зарегистрироваться онлайн на национальном портале, прежде чем входить в систему с помощью опции "Регистрация пользователя". Онлайн- учетные данные пользователя, предоставленные в рамках процесса регистрации Пользователя, потребуются гражданину для входа на национальный портал.
2.	Национальный портал проверяет подлинность учетных данных пользователя в пользовательском репозитории в LDAP. Если проверка подлинности завершается неудачей, портал возвращает сообщение об ошибке. Если аутентификация прошла успешно, пользователю разрешается войти на национальный портал, чтобы воспользоваться государственной электронной услугой.
3.	Пользователь выбирает сервис "Избирательная комиссия -Регистрация избирателей" и выбирает онлайн- заявку на регистрацию избирателя. Пользователю будет представлена онлайн-форма регистрации избирателей. Пользователь заполняет онлайн-форму с соответствующей требуемой информацией и отправляет онлайн-форму.

Шаг	Описание шага
НЕТ	
4.	<p>После отправки портал преобразует данные онлайн-формы, полученные в формате xml-сообщения который отправляется прослушивающему сервлету, запущенному на сервере портала. Сервлет обработает запрос и, в свою очередь, <b>вызовом для отправки формы</b> <code>SubmitVotersRegistration</code> пользователю для определенного пользователем прокси-сервера портала будет добавлен в качестве заголовка сообщения.</p> <p>Данные формы и учетные данные пользователя citizen будут переданы в качестве запросов на ввод веб-службой и будут частью тела сообщения.</p> <p>Экземпляр портала, развернутый в GIDC, попытается установить соединение с центральным Mule инфраструктурой ESB на основе соответствующих учетных данных безопасности аутентификации для вызова веб-службы <code>-SubmitVotersRegistration</code>.</p>
5.	<p>Mule проверяет подлинность идентификатора пользователя и пароля, указанных в профиле токена имени пользователя, переданном экземпляром портала в репозитории пользователей LDAP.</p> <p>Если профиль токена имени пользователя недействителен, Mule обработает исключение и вернет сообщение об ошибке сообщение возвращается на портал.</p> <p>Если маркер имени пользователя действителен, Mule проверит, авторизован ли профиль пользователя соответствующий веб-сервис. Если профиль пользователя не авторизован для доступа к веб-службе, Mule вернет порталу сообщение об ошибке. Если профиль токена имени пользователя действителен и авторизован для доступа к веб-службе, Mule продолжит дальнейшую обработку запроса, как указано в Шаге 6.</p> <p>Mule <code>-EC Services</code>, который <b>действует как прокси для базовой веб-службы</b> <code>-SubmitVotersRegistration</code>,</p>
6.	<p>развернутый на сервере ЕС, будет развернут в экземпляре Mule 1. Этот прокси-сервис будет зарегистрирован в реестре Galaxy. Mule вызовет службы "EC services", развернутые в экземпляре Mule instance 1, посредством обнаружения службой уже зарегистрированной службы "SubmitVotersRegistration" в реестре Galaxy.</p> <p>Mule proxy - Служба EC установит соединение с веб-сервером ЕС конкретного подразделения на котором размещена система регистрации избирателей и веб-служба</p>
7.	<p><code>SubmitVotersRegistration</code> Будет вызвана веб-служба <code>SubmitVotersRegistration</code>, размещенная на сервере ЕС. Онлайн -запрос инициированный с национального портала, поступит на сервер департамента через ESB на базе Mule шлюз предоставления услуг Веб-служба</p>
8.	<p>EC <code>SubmitVotersRegistration</code> обработает данные формы, предоставленные гражданином, и сохранит данные в хранилище данных.</p>
9.	<p>Подтверждение онлайн-заявки с контрольным номером / application number будет возвращено как часть обратного ответа Mule <code>-EC Service</code></p>
10.	<p>Служба Mule EC, развернутая в экземпляре Mule 1, вернет ответ, предоставленный ЕС службой, обратно на сервер портала</p>
11.	<p>Детали аудита транзакции сохраняются в хранилище данных портала</p> <p>Портал отображает ответ онлайн гражданину, предоставляющему контрольный номер / регистрационный номер заявки для отслеживания статуса онлайн-заявки</p>
12.	

2: EC обрабатывает запрос на регистрацию избирателей, и сотрудники Министерства иностранных дел проверяют профиль избирателей



Mule based ESB Service Delivery Gateway

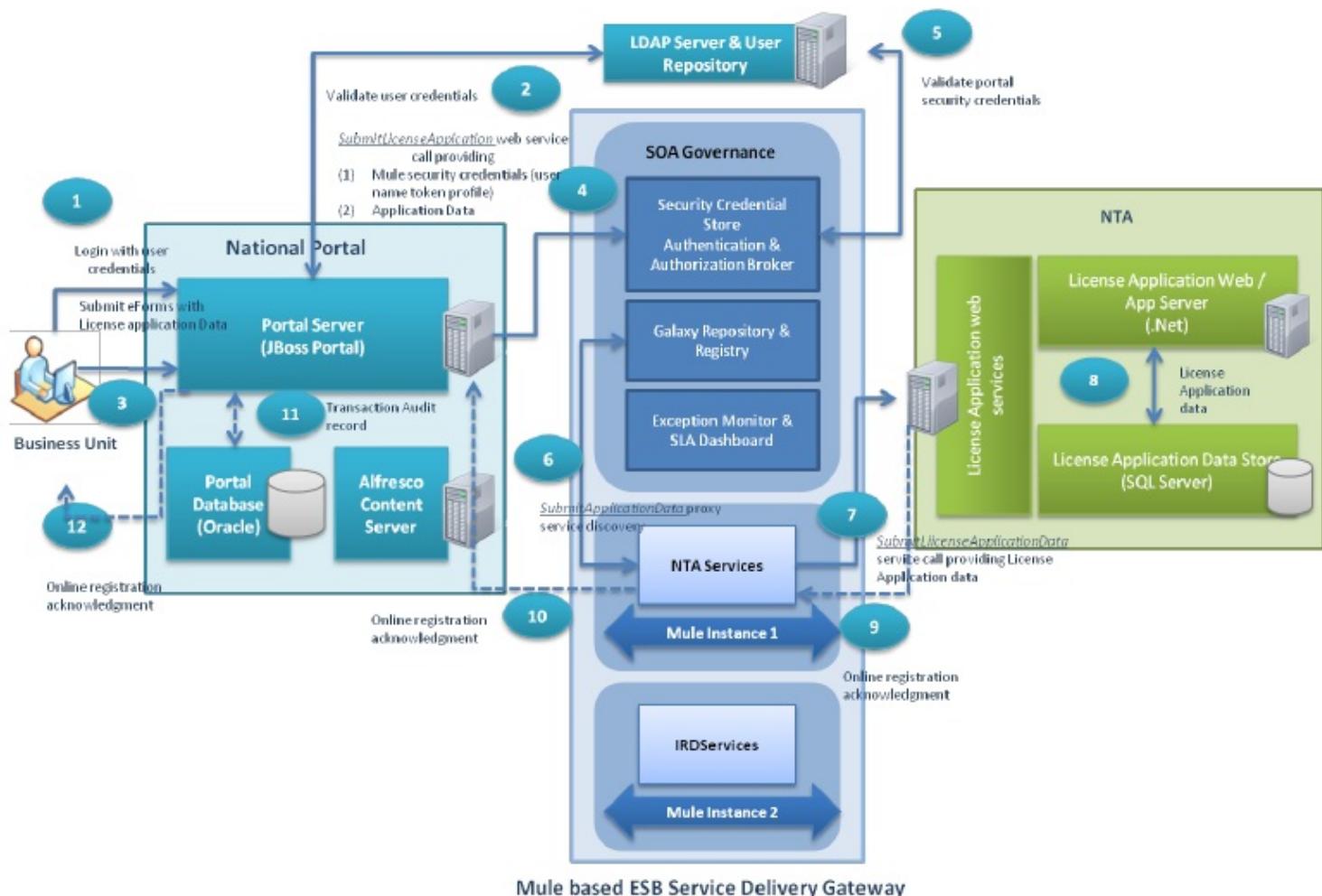
Шаг	Описание шага
1.	Сотрудники департамента EC входят в приложение для конкретного департамента, чтобы просмотреть регистрационные данные онлайн-избирателей, предоставленные гражданином в предыдущем варианте использования
2.	Данные запроса на обслуживание регистрации избирателей для гражданина, занесенные в базу данных EC, извлекаются с сервера EC и отображаются сотрудникам.
3.	<p>В рамках проверки данных о гражданстве избирателей, предоставленных гражданином, конкретный департамент</p> <p>приложение попытается вызвать веб-службу "GetCitizenshipCertificate". Маркер имени пользователя для прокси-сервера EC, определенный пользователем, будет добавлен в качестве заголовка сообщения. Имя гражданина и номер гражданства будут переданы, поскольку запросы на ввод данных веб-службы будут частью тела сообщения.</p> <p>Экземпляр приложения EC, развернутый на сервере EC, попытается установить интеграционную инфраструктуру ESB на основе Mule с соответствующими учетными данными безопасности аутентификации (профиль токена имени пользователя) для вызова веб-службы "GetCitizenshipCertificate".</p>

Шаг НЕТ	Описание шага
4.	<p>Mule проверит подлинность идентификатора пользователя и пароля, указанных в переданном профиле токена имени пользователя экземпляром приложения EC в репозитории пользователей LDAP. Если профиль токена имени пользователя недействителен, Mule обработает исключение и вернет ошибку</p> <p>отправьте ответное сообщение в приложение EC.</p> <p>Если маркер имени пользователя действителен, Mule проверит, авторизован ли профиль пользователя соответствующий веб-сервис. Если профиль пользователя не авторизован для доступа к для доступа к веб-сервису, Mule вернет сообщение об ошибке обратно в приложение EC.</p> <p>Если профиль токена имени пользователя действителен и авторизован для доступа к веб-службе, Mule продолжит дальнейшую обработку запроса</p>
5.	<p>Mule -Службы сертификатов гражданства, которые действуют как прокси для базовой веб-службы -GetCitizenshipCertificate, развернутые на сервере MoNA, будут развернуты в экземпляре Mule 2. Этот прокси-сервис будет зарегистрирован в реестре Galaxy</p> <p>Mule вызовет "Службы сертификатов гражданства", развернутые в экземпляре Mule 2, посредством обнаружения службой уже зарегистрированной службы "GetCitizenshipCertificate" в реестре Galaxy . Mule proxy -службы</p>
6.	<p>получения сертификата гражданства установит соединение с Министерством здравоохранения сервер, относящийся к конкретному ведомству, на котором размещен веб-сервис GetCitizenshipCertificate. Будет вызван веб-сервис GetCitizenshipCertificate, размещенный на сервере MoNA. Онлайн-запрос, инициированный из приложения EC, поступит на сервер департамента министерства здравоохранения через шлюз доставки услуг ESB на основе Mule Веб-служба обработает запрос, получив доступ к хранилищу данных департамента, которое фиксирует сведения о гражданстве. Если найдена соответствующая запись для конкретного имени гражданина и номера гражданства, запись является извлекается и возвращается как часть выходного ответа обратно в Mule -Сертификат гражданства ServicesII. Если соответствующая запись не найдена, веб-служба вернет соответствующее сообщение об ошибке. Mule</p>
7.	<p>-Службы сертификатов гражданства, развернутые в экземпляре Mule 2, вернут ответ обратно на вызывающий веб-сервер EC / сервер приложений</p>
8.	<p>Сотрудник Министерства иностранных дел входит в приложение для конкретного департамента Министерства иностранных дел с учетными данными пользователя, чтобы проверить профиль избирателя в заявлении на получение паспорта.</p>
9.	<p>Сотрудники Министерства иностранных дел выбирают возможность проверить профиль заявителя на получение паспорта избирателя и отправляют запрос</p>
10.	<p>В рамках получения данных профиля избирателей приложение, относящееся к конкретному подразделению, попытается вызвать веб-службу "GetVotersProfile" Маркер имени пользователя для определенного пользователем прокси-сервера MoFA будет добавлен в качестве заголовка сообщения Экземпляр приложения MoFA, развернутый на сервере MoFA, попытается установить соединение с инфраструктурой ESB на базе центрального Mule с соответствующими учетными данными безопасности аутентификации (user профиль маркера имени пользователя) для вызова веб-службы "GetVotersProfile"</p>
11.	<p>Mule проверяет подлинность идентификатора пользователя и пароля, указанных в профиле токена имени пользователя, переданным экземпляром приложения MoFA в репозитории пользователей LDAP. Если профиль токена имени пользователя недействителен, Mule обработает исключение и вернет сообщение об ошибке обратно в приложение MoFA.</p>

Шаг	Описание шага
НЕТ	
	<p>Если маркер имени пользователя действителен, Mule проверит, авторизован ли профиль пользователя для доступа к соответствующему веб-сервису. Если профиль пользователя не авторизован для доступа к веб-службе, Mule вернет сообщение об ошибке обратно в приложение MoFA.</p> <p>Если профиль токена имени пользователя действителен и ему разрешен доступ к веб-службе, Mule продолжит дальнейшую обработку запроса</p>
12.	<p>Mule -EC ServicesII, который действует как прокси для базовой веб-службы -GetVotersProfileII , развернутый на сервере EC, будет развернут в экземпляре Mule 1. Этот прокси-сервис будет зарегистрирован в Реестре Galaxy Mule вызовет службы "EC Services", развернутые в экземпляре Mule instance 1, посредством обнаружения службой уже зарегистрированной службы "GetVotersProfile" в реестре Galaxy.</p>
13.	<p>Mule proxy -EC ServicesII установит соединение с сервером, специфичным для отдела EC, который размещает веб-службу GetVotersProfile. Будет вызвана веб-служба GetVotersProfile, размещенная на сервере EC. Инициирован онлайн-запрос из MoFA приложение попадет на сервер департамента EC через ESB на базе Mule шлюз предоставления услуг Веб-служба обработает запрос на доступ к хранилищу данных о гражданах страны избирателя</p>
14.	<p>Службы Mule -EC,II развернутые в экземпляре Mule 1, вернут ответ обратно вызывающему веб -серверу / серверу приложений MoFA</p>
15.	<p>Регистрационные данные избирателей отображаются сотрудникам Министерства иностранных дел</p>

#### Сценарий использования 3: Процесс онлайн-регистрации лицензии VAS

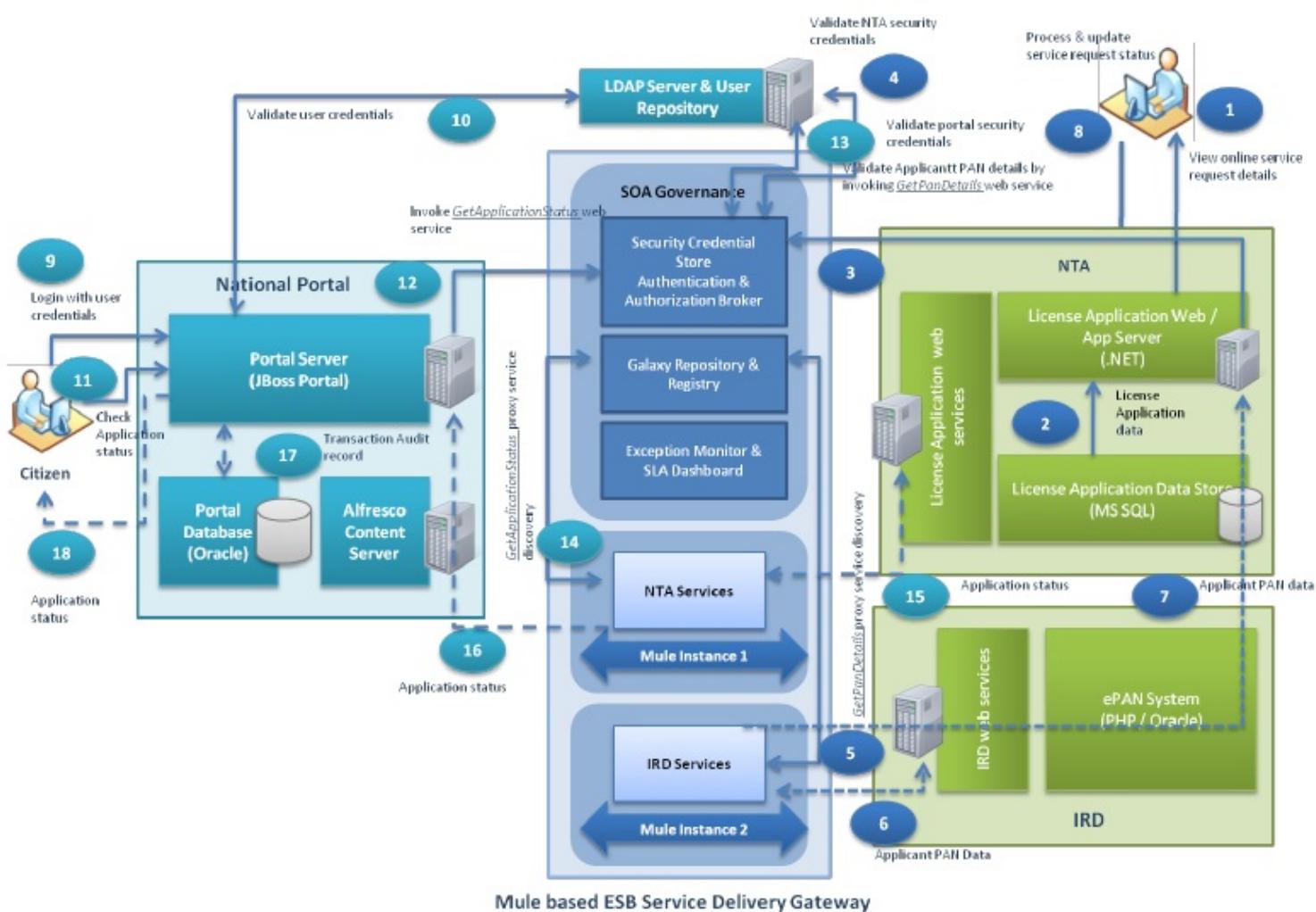
1: Предприятие отправляет онлайн-запрос на регистрацию лицензии VAS с Национального портала



Шаг	Описание шага
1.	Бизнес входит в систему Национального портала с учетными данными пользователя. Бизнесу потребуется зарегистрироваться онлайн на национальном портале до входа в систему с помощью опции "Регистрация пользователя". Учетные данные онлайн-пользователя, предоставленные в рамках процесса регистрации Пользователя, потребуются гражданину для входа на национальный портал.
2.	Национальный портал проверяет подлинность учетных данных пользователя в пользовательском репозитории в LDAP. Если проверка подлинности завершается неудачей, портал возвращает сообщение об ошибке. Если аутентификация прошла успешно, пользователю разрешается войти на национальный портал, чтобы воспользоваться государственной электронной услугой.
3.	Пользователь выбирает сервис NTA -VAS License Registration   Es и выбирает онлайн-заявку на регистрацию лицензии VAS. Пользователю будет представлена онлайн-форма регистрации лицензии Пользователь заполняет онлайн-форму с соответствующей требуемой информацией и отправляет онлайн-форму
4.	После отправки портал преобразует собранные данные онлайн-формы в формат xml-сообщения, которое отправляется прослушивающему серверу, запущенному на сервере портала. Сервлет обработает запрос и, в свою очередь, вызовет веб-службу "SubmitLicenseApplication" для отправки информации. Маркер имени пользователя для определенного пользователем прокси-сервера портала будет добавлен в качестве заголовка сообщения.

Шаг	Описание шага
НЕТ	
	<p>Данные формы и учетные данные бизнес-пользователя будут переданы в качестве запросов на ввод веб-службой и будут частью текста сообщения. Экземпляр портала, развернутый в GIDC, попытается установить соединение с центральным Mule инфраструктурой ESB на основе соответствующих учетных данных безопасности аутентификации для вызова <code>-SubmitLicenseApplication()</code> веб-службы</p>
5.	<p>Mule проверяет подлинность идентификатора пользователя и пароля, указанных в профиле токена имени пользователя, переданном экземпляром портала в репозитории пользователей LDAP. Если профиль токена имени пользователя недействителен, Mule выполнит ожидание и вернет сообщение об ошибке</p> <p>сообщение возвращается обратно на портал.</p> <p>Если маркер имени пользователя действителен, Mule проверит, авторизован ли профиль пользователя соответствующий веб-сервис. Если профиль пользователя не авторизован для доступа к для доступа к веб-службе, Mule вернет порталу сообщение об ошибке. Если профиль токена имени пользователя действителен и авторизован для доступа к веб-службе, Mule продолжит дальнейшую обработку запроса, как указано в шаге 6</p> <p>Mule -NTA Services(), который действует как прокси для базовой веб-службы <code>-SubmitLicenseApplication()</code>,</p>
6.	<p>развернутый на сервере NTA, будет развернут в экземпляре Mule 1. Этот прокси-сервис будет зарегистрирован в реестре Galaxy. Mule вызовет "Службы NTA", развернутые в экземпляре Mule instance 1, посредством обнаружения службой уже зарегистрированной службы <code>SubmitLicenseApplication()</code> в реестре Galaxy.</p> <p>Mule proxy -Служба NTA установит соединение с веб-сервером NTA конкретного подразделения на котором размещена система регистрации лицензий VAS и веб-служба</p>
7.	<p><code>SubmitLicenseApplication</code> Будет вызвана веб-служба <code>SubmitLicenseApplication</code>, размещенная на сервере NTA. Онлайн запрос, инициированный с национального портала, поступит на сервер департамента через шлюз доставки услуг ESB на основе Mule Веб-служба NTA <code>SubmitLicenseApplication</code> обработает</p>
8.	<p>данные формы, предоставленные предприятием, и сохранит их в хранилище данных.</p>
9.	<p>Подтверждение онлайн-заявки с контрольным номером / application number будет возвращено как часть обратного ответа Mule -службе NTA</p>
10.	<p>Служба Mule NTA, развернутая в экземпляре Mule 1, вернет ответ, предоставленный службой DoTM, обратно на сервер портала</p>
11.	<p>Сведения об аудите транзакции сохраняются в хранилище данных портала</p>
12.	<p>Портал отображает онлайн-ответ компании, предоставляющей контрольный номер / регистрационный номер заявки для отслеживания статуса онлайн-заявки</p>

2: НТА обрабатывает запрос на обслуживание для регистрации лицензии VAS и проверяет статус регистрации гражданина на Национальном портале



Шаг	Описание шага
Шаг НЕТ	
1.	Сотрудники отдела NTA входят в приложение для конкретного отдела, чтобы просмотреть онлайн-информацию о регистрации лицензии VAS , предоставленную предприятием в предыдущем варианте использования
2.	Подробная информация о запросе на обслуживание для регистрации лицензии для бизнеса, хранящаяся на сервере базы данных NTA , извлекается и отображается сотрудникам NTA.

Шаг	Описание шага
НЕТ	
4.	Mule проверяет подлинность идентификатора пользователя и пароля, указанных в переданном профиле токена имени пользователя экземпляром приложения NTA в репозитории пользователей LDAP. Если профиль токена имени пользователя недействителен, Mule обработает исключение и вернет ошибку отправьте ответное сообщение приложению NTA. Если маркер имени пользователя действителен, Mule проверит, авторизован ли профиль пользователя соответствующий веб-сервис. Если профиль пользователя не авторизован для доступа к веб-службе, Mule вернет сообщение об ошибке обратно в приложение NTA. Если профиль токена имени пользователя действителен и авторизован для доступа к веб-службе, Mule продолжит дальнейшую обработку запроса Mule -IRD Services, который действует как прокси для базовой веб-службы -GetPANDetails, развернутый на IRD сервере, будет развернут в экземпляре Mule 2. Этот прокси-сервис будет зарегистрирован в реестре Galaxy Mule вызовет "Службы IRD", развернутые в экземпляре Mule 2, посредством обнаружения службой уже зарегистрированной службы "GetPANDetails" в реестре Galaxy. Mule proxy -IRD Services установит соединение с сервером, относящимся к конкретному отделу IRD, который размещает веб-службу GetPANDetails
5.	Будет вызвана веб-служба GetPANDetails, размещенная на сервере IRD. Инициирован онлайн-запрос
6.	из NTA приложение попадет на сервер IRD department через ESB на основе Mule шлюз предоставления услуг Веб-служба обработает запрос на доступ к хранилищу данных отдела, которое фиксирует детали бизнес-кастюоли.
7.	Службы Mule -IRD, развернутые в экземпляре Mule 2, вернут ответ обратно вызывающему веб-серверу / серверу приложений NTA
8.	Сотрудники NTA проверят возвращенный ответ и продолжат обработку запроса на регистрацию лицензии VAS . На различных этапах обработки запроса онлайн-сервиса на регистрацию лицензии сотрудники NTA обновят статус заявки.
9.	Предприятие, чтобы проверить статус своей онлайн-регистрации лицензии, войдет в систему на Национальном портале с учетными данными пользователя. Учетные данные онлайн-пользователя, предоставленные в рамках процесса регистрации пользователя, потребуются предприятию для входа на национальный портал.
10.	Национальный портал проверяет подлинность учетных данных пользователя в пользовательском репозитории в LDAP. Если проверка подлинности завершается неудачей, портал возвращает сообщение об ошибке Если аутентификация прошла успешно, бизнес-пользователю разрешено войти в национальный портал, чтобы воспользоваться правительство. электронные услуги
11.	Пользователь выбирает опцию NTA -VAS License Registration Status eService. Пользователь вводит регистрационный номер онлайн и название компании / регистрационный номер и отправляет запрос для проверки текущего состояния онлайн-регистрации, инициированной в предыдущем варианте использования После отправки портал преобразует собранные онлайн-данные в формат xml-сообщения, который
12.	отправляется прослушивающему сервлету, запущенному на сервере портала. Сервлет обработает запрос и, в свою очередь, вызовет веб-службу "GetVASApplicationStatus"

Шаг	Описание шага
НЕТ	
	<p>предоставить информацию. Маркер имени пользователя для определенного пользователем прокси-сервера портала будет добавлен в качестве заголовка сообщения.</p> <p>Критерии поиска и учетные данные пользователя-гражданина будут переданы в качестве входных данных веб-службы</p> <p>запрашивает и будет частью тела сообщения.</p> <p>Экземпляр портала, развернутый в GIDC, попытается установить соединение с центральным Mule инфраструктурой ESB на основе соответствующих учетных данных безопасности аутентификации для вызова -GetVASApplicationStatus- веб-службы</p>
13.	<p>Mule проверяет подлинность идентификатора пользователя и пароля, указанных в профиле токена имени пользователя, переданном экземпляром портала в репозитории пользователей LDAP.</p> <p>Если профиль токена имени пользователя недействителен, Mule выполнит ожидание и вернет сообщение об ошибке</p> <p>сообщение возвращается на портал.</p> <p>Если маркер имени пользователя действителен, Mule проверит, авторизован ли профиль пользователя соответствующий веб-сервис. Если профиль пользователя не авторизован для доступа к веб-службе, Mule вернет порталу сообщение об ошибке. Если профиль токена имени пользователя действителен и авторизован для доступа к веб-службе, Mule продолжит дальнейшую обработку запроса Mule</p> <p>-NTA Services-, который действует как прокси для базовой веб-службы</p>
14.	<p>-GetVASApplicationStatus-, развернутый на сервере NTA, будет развернут в экземпляре Mule 1.</p> <p>Этот прокси-сервис будет зарегистрирован в реестре Galaxy Mule</p> <p>вызовет "Службы NTA", развернутые в экземпляре Mule 1, посредством обнаружения службой уже зарегистрированной службы "GetVASApplicationStatus" в реестре Galaxy. Mule proxy -NTA Services- установит соединение с сервером, специфичным для отдела NTA, который размещает веб-службу GetVASApplicationStatus</p>
15.	<p>Будет вызвана веб-служба GetVASApplicationStatus, размещенная на сервере NTA. Онлайн</p> <p>запрос, инициированный с национального портала, поступит на сервер департамента NTA через Mule</p> <p>основанный на ESB шлюз доставки услуг. Веб-служба обработает запрос, обращаясь к хранилищу данных отдела, которое фиксирует сведения о регистрации лицензии</p>
16.	<p>Служба Mule NTA, развернутая в экземпляре Mule 1, вернет ответ, предоставленный службой NTA, обратно на сервер портала</p>
17.	<p>Сведения об аудите транзакции сохраняются в хранилище данных портала</p>
18.	<p>Портал отображает ответ компании с обновлением статуса, если таковой имеется.</p>

#### 7.2.4 Анализ пробелов

Пробел - это сама цель с отсутствием какой-либо интеграции между отделами и платформами.

## 7.2.5 Дорожная карта архитектуры интеграции

Дорожная карта высокого уровня представляет последовательность в приоритете реализации проектных решений. Упомянутые здесь этапы имеют разные временные рамки в соответствии со стратегическими планами клиента. Это просто последовательные этапы реализации.

### Этап А

1. NGSDG обеспечит поддержку сервис-ориентированной архитектуры (SOA) и будет действовать как корпоративная сервисная шина для всех взаимодействий между потребителями услуг (гражданами и предприятиями) и различными поставщиками услуг (правительственными ведомствами) и даже между правительственными ведомствами. Корпоративная служебная шина SDG в качестве промежуточного программного обеспечения обеспечивает бесперебойную совместимость и облегчит простой обмен данными и событиями между подразделениями,
2. позволяя обслуживать устаревшие приложения - с помощью NGSDG устаревшие приложения могут предлагать свои услуги различным другим потребителям, подключенным к корпоративной служебнойшине.
3. Обеспечьте общий набор интеграционных спецификаций и единую точку доступа.
4. Безопасность и аудит - Обеспечивает лучшее отслеживание (аудит) и безопасность каждого вызова службы и обеспечивает государственный контроль с помощью полных журналов аудита и временной отметки транзакций.

### Фаза В

Предоставляет необходимые соединители для взаимодействия с приложениями, разработанными на уровне подразделения. 1. 2. Способен обрабатывать большое количество транзакций по всей сети, 3. 4. Обеспечивает миграцию и преобразование формата, если такие имеются, наряду с маршрутизацией и фильтрацией данных. межведомственных операций в режиме реального времени или почти в режиме реального времени. работа, отслеживание всех транзакций правительства Непала.

### Фаза С

1. Общие сервисы - В будущем SDG Enterprise Service Bus сможет добавлять дополнительные функциональные возможности для поддержки общих сервисов, таких как аутентификация, интерфейс платежного шлюза, службы коротких сообщений, службы мгновенных сообщений и т.д.

Ссылка: Для подробного описания каждого элемента архитектуры интеграции обратитесь к GEA Enterprise Architecture continuum и репозиторию архитектуры. Обратитесь к "Руководству по проектированию ESB для GEA - SOA в Непале" и "Руководству по разработке GEA - SOA в Непале" для получения подробной информации, относящейся к архитектуре интеграции

## 7.3 Архитектура безопасности

### 7.3.1 Принципы архитектуры безопасности

#### Принцип # 1

##### Имя

Соответствие требованиям, отбор и стандартизация средств контроля безопасности

<b>Заявление</b>	<p>Средства контроля безопасности должны соответствовать заранее определенным политикам безопасности.</p> <p>Выбор средств контроля безопасности должен основываться на анализе рисков и решении по управлению рисками . Процесс выбора новых средств контроля будет учитывать как степень снижения рисков, обеспечиваемую средствами контроля, так и общие затраты на приобретение, внедрение и поддержание средств контроля.</p> <p>Выбор средств контроля должен определяться способностью их единобразного применения по всему предприятию и минимизировать исключения.</p>
<b>Обоснование</b>	<p>Создание среды, основанной на стандартах, снизит эксплуатационные расходы., улучшение интероперабельности и возможности поддержки</p> <p>Обеспечивает соответствие решений безопасности назначению</p> <p>Предотвращает нарушения конфиденциальности</p>
<b>Последствия</b>	Политика ИТ-безопасности, политика защиты данных и безопасность приложений должны разрабатываться для всех этапов

<b>Принцип № 2</b>	
<b>Имя</b>	Уровни безопасности
<b>Заявление</b>	Информационные системы (включая приложения, вычислительные платформы, данные и сети) будут поддерживать уровень безопасности, соизмеримый с риском и масштабами ущерба, который может возникнуть в результате потери, неправильного использования, раскрытия или модификации информации.
<b>Обоснование</b>	С практической точки зрения абсолютная безопасность не может быть достигнута ни в одной информационной системе. Следовательно, будут применены меры контроля безопасности для снижения риска до приемлемого уровня.
<b>Последствия</b>	Необходимо сформировать отдельные централизованные группы для обеспечения безопасности приложений, данных и ИТ. Для этого необходимо поддерживать репозиторий.

<b>Принцип № 3</b>	
<b>Имя</b>	Измерение безопасности
<b>Заявление</b>	Средства контроля безопасности можно будет пересматривать или проводить аудит с помощью некоторых качественных или количественных средств для отслеживания и обеспечения поддержания риска на приемлемом уровне.
<b>Обоснование.</b>	Позволяет исправлять ошибки и сводить к минимуму неправильное использование системы
<b>Последствия</b>	Необходимо определить структуру отчетности, и руководство должно иметь возможность просматривать консолидированный отчет

<b>Принцип № 4</b>	
<b>Имя</b>	Использование обычной аутентификации пользователя
<b>Заявление</b>	Необходимо поддерживать использование общей системы аутентификации пользователей на всех уровнях GEA . Это включает повторное использование той же системы аутентификации для национального портала

	сервисы входа в систему и регистрации на автобусе, как для потребителей, так и для производителей.
<b>Обоснование</b>	Обеспечивает легкий доступ к авторизованным пользователям Такой подход позволяет избежать дублирования усилий и обеспечивает экономию за счет масштаба
<b>Последствия</b>	Необходимо разработать механизм централизованной аутентификации. Необходимо изменить существующие приложения, чтобы они могли использовать централизованную модель.

### 7.3.2 Базовая архитектура безопасности.

Целью структуры архитектуры безопасности является поддержка организаций и администраторов в предоставлении электронных услуг предприятиям и гражданам посредством соответствующих механизмов выбора для аутентификации и регистрации пользователей. Принятие директив и руководящих принципов Системы безопасности повысит уровень безопасности услуг, предоставляемых органами государственного управления, что позволит улучшить общее функционирование правительства. Система безопасности является важным аспектом стратегии правительства Непала по переходу и адаптации услуг к требованиям действующих отраслевых стандартов. В текущем сценарии в Непале нет единой политики безопасности, которой следуют все департаменты.

### 7.3.3 Целевая архитектура безопасности.

Правительство Непала вынуждено менять подходы к ведению бизнеса под влиянием многих факторов как внутренних, так и внешних. Для поддержки этого роста и изменений безопасность должна быть интегрирована в бизнес-процессы. Основываясь на тенденциях в области безопасности, а также на анализе и наблюдениях за текущим состоянием правительства Непала, правительство Непала должно сформулировать последовательный подход к обеспечению информационной безопасности в окружающей среде. Для удовлетворения потребностей в обеспечении безопасности предприятия правительственная архитектура безопасности Непала обеспечивает базовую основу для подхода к обеспечению безопасности при сохранении согласованности на всем предприятии. Основными целями ESA являются:

Определите параметры безопасности  
Сосредоточьте усилия по обеспечению безопасности на обеспечении надлежащего контроля для адекватной защиты информационных активов на основе бизнес-факторов; Создайте в организации сообщество безопасности с общим языком и подходом; Создайте структуру безопасности, чтобы интегрировать ее в общий бизнес-контекст; и предоставьте бизнес-подразделениям дорожную карту с указанием приоритетов для продвижения к этой общей модели.

Архитектура корпоративной безопасности преобразует бизнес-цели в людей, процессы и технологии, компоненты, необходимые для защиты информации, активов и предоставления правительству Непала структурированной, ориентированной на бизнес программы безопасности. ESA состоит из конкретных критерий для каждого бизнес-подразделения для определения областей сосредоточения, ролей и обязанностей по поддержке общей функции обеспечения безопасности и стратегического подхода к миграции. Кроме того, ESA демонстрирует тот факт, что информационная безопасность - это не только технологический вопрос. Не существует надежного технического решения для внедрения архитектуры безопасности на таком крупном предприятии, как правительство Непала. Для достижения полной зрелости технологии должны сочетаться с эффективными процессами и квалифицированным персоналом.

В целом аспекты безопасности можно разделить на пять различных разделов

Политика безопасности: Безопасность информационных технологий относится к процессам и методологиям, которые разработаны и внедрены для защиты печатной, электронной или любой другой формы конфиденциальной, частной и чувствительной информации или данных от несанкционированного доступа, использования, неправильного использования, раскрытия, уничтожения,

изменение или сбой. Информационная безопасность связана с конфиденциальностью, целостностью и доступностью данных независимо от того, какую форму они могут принимать: электронную, печатную или иную.

Безопасность данных: Проще говоря, безопасность данных - это практика обеспечения защиты данных от повреждения и несанкционированного доступа. В основе безопасности данных лежит обеспечение конфиденциальности при одновременной защите данных.

Данные считаются основным активом и как таковые должны быть защищены способом, соизмеримым с их ценностью. Безопасность и конфиденциальность должны быть сосредоточены на контроле несанкционированного доступа к данным. Нарушения безопасности могут поставить под угрозу нашу способность предоставлять услуги; привести к потере доходов из-за мошенничества или уничтожения личных или конфиденциальных данных.

Безопасность приложений: Безопасность приложений - это использование программного обеспечения, аппаратных средств и процедурных методов для защиты приложений от внешних угроз. Встроенные в приложения меры безопасности и продуманная процедура обеспечения безопасности приложений сводят к минимуму вероятность того, что хакеры смогут манипулировать приложениями и получать доступ, красть, изменять или удалять конфиденциальные данные. Принципы безопасности приложений - это совокупность желательных свойств приложения, моделей поведения, дизайна и практик внедрения, которые направлены на снижение вероятности реализации угрозы и воздействия, если эта угроза будет реализована.

Принципы безопасности - это независимые от языка, архитектурно нейтральные примитивы, которые могут быть использованы в большинстве методологий разработки программного обеспечения для проектирования и конструирования приложений.

Безопасность инфраструктуры

Управление безопасностью: Управление информационной безопасностью обеспечивает процессы управления и гарантии, позволяющие бизнес-подразделениям гарантировать, что бизнес-транзакциям можно доверять; гарантировать, что ИТ-сервисы пригодны для использования и могут противостоять сбоям и восстанавливаться после сбоев из-за ошибок, атак или стихийных бедствий; и гарантировать, что критически важная конфиденциальная информация скрывается от тех, кто не должен иметь к ней доступа

### 7.3.3.1 Политика безопасности

Информационная безопасность повышает ценность организации только в контексте бизнеса. Бизнес-цели определяют требования к безопасности; безопасность может способствовать достижению бизнес-целей за счет эффективного и результативного управления рисками. Необходимо поддерживать баланс между стремлением к достижению агрессивных бизнес-целей и способностью управлять рисками, влияющими на бизнес. Подход к обеспечению информационной безопасности для правительства Непала должен быть гибким, учитывать рынок и бизнес и приводить к эффективной и экономичной инфраструктуре безопасности.

Информационные технологии подразделяются на девять различных компонентов безопасности -

Организация;  
Соблюдение нормативных требований; Управление политиками; Осведомленность о безопасности;  
Измерение и отчетность;  
Управление информационными и технологическими активами; Реагирование на инциденты; Управление угрозами и уязвимостями;  
и управление идентификацией.

### 7.3.3.2 Безопасность данных

Логическая безопасность данных обычно относится к управлению людьми, процессами и процедурами, необходимыми для создания согласованного корпоративного представления данных организации с целью повышения безопасности данных.

Более конкретно, согласно Институту управления данными, это - система прав на принятие решений и ответственности за процессы, связанные с информацией, выполняемые в соответствии с согласованными моделями, которые описывают, кто какие действия может предпринимать с какой информацией и когда, при каких обстоятельствах, с использованием каких методов.||

Логическая защита данных помогает организовать передачу данных простым и продуктивным способом. Основной целью этого мероприятия является архивирование, по крайней мере, следующего:

- Обеспечение более эффективного принятия решений
- Уменьшение операционных трудностей
- Защита потребностей заинтересованных сторон в данных
- Обучить руководство и персонал принятию общих подходов к решению проблем с данными
- Выстраивать стандартные, воспроизводимые процессы
- Снижать затраты и повышать эффективность за счет координации усилий
- Обеспечивать прозрачность процессов

Для архивирования этого должна быть четко определенная политика контроля доступа. Когда пользователь пытается получить доступ к одному бизнесу сервис, процесс контроля доступа должен проверить, что пользователь был авторизован для использования этого ресурса. Служебная матрица авторизации может определять этот контроль доступа и формировать базу правил для системы, позволяющую решать, должен ли быть предоставлен запрос доступа от пользователя или отклонен. Ниже приведен пример из электронной таблицы матрицы авторизации сервиса .

Nepal GEA - Service Authorization								
Service Provider	Business Service ID	Business Service Name	Web Service ID	Web Service Name	Web Service Description	Type of Service	Actor	Class of Roles[Job Process]
IRD (e-PAN)	BA_BS_01	Issue of PAN to a person	BA_WS_01	Apply for PAN	This web service will allow citizens to apply for PAN online. This web service is already available via Website	G2C	Citizen	Applicant
			BA_WS_02	Know Registration Status	This web service will allow citizens to know the PAN registration status. This service is already available via SMS	G2C	Citizen	Applicant
			BA_WS_03	Get Taxpayer's Details	This web service to be used by citizens will provide the taxpayer's PAN details namely the PAN, taxpayer's name, address etc.	G2C	Citizen	Tax Payer
			BA_WS_03	Get Taxpayer's Details	This web service will be used by the govt. unit / agency who would like to validate the taxpayer's PAN details	G2G	Govt Agency(non IRD)	Section Officer Sakha Adhikari  or Above

### 7.3.3.3 Безопасность приложения

#### Структура аутентификации

Целью системы электронной аутентификации является поддержка организаций и администраторов в предоставлении электронных услуг предприятиям и гражданам посредством соответствующих механизмов отбора для аутентификации и регистрации пользователей. Принятие директив и руководящих принципов Системы электронной аутентификации повысит уровень безопасности услуг, предоставляемых органами государственного управления, что позволит улучшить общее функционирование правительства. Система электронной аутентификации является важным аспектом стратегии правительства Непала по переходу и адаптации услуг к требованиям действующих отраслевых стандартов. Система электронной аутентификации требует соблюдения требований всеми организациями, участвующими в предоставлении услуг электронного правительства, для создания безопасной и надежной среды для надлежащего обращения с ними через Интернет.

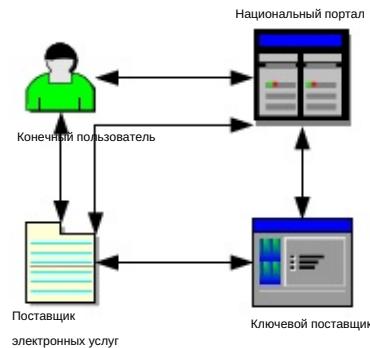


Рисунок Общая архитектура GEA - e-Authentication Framework

Таким образом, агентства предлагают свои услуги через Национальный портал или напрямую, установлен уровень доверия, аутентификации и регистрации. Конечные пользователи пользуются предлагаемыми онлайн-сервисами после прохождения тестирования и проверки точности своей электронной идентификации.

#### **Основные принципы и содержание системы электронной аутентификации**

Основным вкладом Системы электронной аутентификации является предоставление конкретных правил и руководств для: Классификации данных, обрабатываемых электронными службами, Определения "уровней достоверности" для электронных служб на основе категории использования данных, но также с учетом возможных последствий, которые могут быть вызваны неправильной эксплуатацией или управлением ими. Взаимосвязь доверия между уровнями, где для каждого уровня аутентификации определены конкретные механизмы аутентификации. Взаимосвязь каждого уровня доверия с соответствующими "процедурами регистрации". Государственные административные органы, которые разрабатывают электронные услуги, должны следовать следующим основным шагам, как предусмотрено в этой Системе электронной аутентификации:

Определите уровень доверия, с которым работает эта служба, предварительно точно определив типы используемых данных

В зависимости от уровня доверия и следуя рекомендациям этого PPSA, выберите соответствующий механизм аутентификации.

В зависимости от уровня доверия и следуя рекомендациям настоящего PPSA, принять необходимые процедуры регистрации для пользователей.

#### **Модель аутентификации**

В контексте eService access пользователи обычно регистрируются в нескольких несвязанных сервисах с разным пользовательским интерфейсом и разными учетными данными. Таким образом, пользователь имеет несогласованный пользовательский интерфейс и работает с разными копиями идентификатора. Платформа электронной аутентификации попытается решить эти проблемы путем сравнения различных моделей аутентификации и анализа того, какая из них лучше всего работает в данном сценарии. В широком смысле мы можем определить три типа систем управления идентификацией: изолированную, централизованную и федеративную модель. Федеративная модель, которая наилучшим образом соответствует требованиям безопасности NGEA, представлена ниже -

#### **Федеративная модель**

Хотя изолированная модель требует нескольких паролей для одного пользователя, централизованную модель сложно реализовать. Баланс между двумя - федеративная модель. Федеративная модель предоставляет единую службу входа в систему для нескольких приложений с единственным идентификатором. В этой модели учетные данные выдаются федеративной центральной службой входа в систему после процесса регистрации. Учетные данные, выданные этой центральной службой входа в систему, могут использоваться другими приложениями. У разных приложений есть свой собственный процесс регистрации пользователя для определения уровня авторизации. Как только процедура аутентификации выполняется Центральной службой входа в систему, она сообщает результат приложению. Одним из преимуществ этой модели является то, что пользователь может сохранять отдельный идентификатор приложения для каждого участвующего приложения. Пока пользователь регистрируется в Центральной службе входа в систему, пользователю будет присвоен новый идентификатор для последующего использования. Служба входа в систему обязана поддерживать соответствие между идентификатором службы централизованного входа в систему и идентификатором каждого приложения. Эта модель может быть реализована для поддержки двух потоков аутентификации:

Служба тщательного централизованного входа в систему

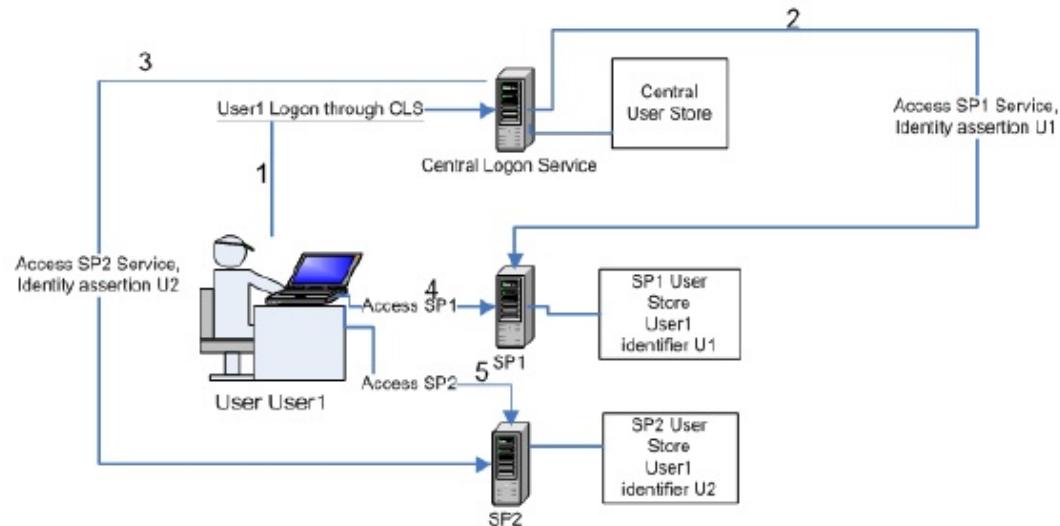
Тщательный вход в приложение

#### **Вход в систему через портал**

В этом потоке пользователь сначала войдет в систему на портале, а затем пользователю будет представлен список сервисов, к которым он / она может получить доступ. После выбора пользователь будет доставлен в соответствующее приложение в качестве аутентифицированного пользователя.

#### **Вход в систему через приложение**

В этом потоке пользователь сначала получает доступ к приложению. Затем приложение обязано аутентифицировать пользователя с использованием учетных данных, специфичных для приложения. Аутентификация на портале здесь не будет играть никакой роли.



#### **7.3.3.4 Безопасность веб-служб**

Веб-сервисы можно рассматривать как интерфейс, доступ к которому осуществляется по протоколу передачи гипертекста (HTTP) и выполняется в удаленной системе, в которой размещается запрошенная услуга. Основным преимуществом веб-сервиса является совместимое межмашинное взаимодействие по сети. Поэтому, независимо от того, является ли он автономным или составным, он должен обеспечивать надежные гарантии безопасности. Безопасность веб-сервисов может быть описана с помощью хорошо известных параметров безопасности, то есть:

Целостность: сообщение должно оставаться неизменным во время передачи через все посреднические службы  
сервисы различного характера. Конфиденциальность:  
Содержимое сообщения нельзя просмотреть во время передачи, кроме как авторизованными сервисами, которым необходимо просмотреть содержимое сообщения для маршрутизации. Доступность: Сообщение должно быть незамедлительно доставлено законные пользователи получатели, на которых они имеют право. предполагаемому получателю, который гарантирует, что

Кроме того, каждый веб-сервис должен защищать свой ресурс от несанкционированного доступа.

Выполнение таких требований требует соответствующих средств идентификации и авторизации. В среде веб-сервисов также важно защищать стороны, которым требуется услуга, чтобы гарантировать, что вся информация, используемая сторонами, является подлинной и правильной.

Основные аспекты безопасности веб-служб можно разделить на следующие подразделы:

SSL / TSL  
Безопасность данных XML  
Язык разметки утверждений безопасности  
Безопасность сообщений SOAP

#### 7.3.4 Анализ

##### пробелов 1.

- Регистрация: Она должна быть простой, и все взаимодействующие приложения и компоненты (база данных, веб-сервер, сервер приложений и пользователи) системы должны регистрироваться, идентифицироваться и проверяться, а все действия должны надежно регистрироваться и авторизовываться единым централизованным способом.
2. Единая точка доступа: Для каждого пользователя должна быть единная точка входа в приложение. Для аутентификации и авторизации пользователей потребуются компоненты идентификации и аутентификации.
3. Идентификация: Процесс идентификации необходим для присвоения уникального идентификатора всем пользователям и компонентам, которые взаимодействуют с системой. Система должна распознавать отдельного пользователя / экземпляр компонента и отличать его от других пользователей / компонентов. Имя пользователя должно быть присвоено всем пользователям приложения. Идентификатор приложения должен быть присвоен всем компонентам и интерфейсным приложениям
4. Аутентификация: Аутентификация - это процесс проверки личности, заявленной пользователем системы / компонентом или для него. Система обязана аутентифицировать пользователя / компонент и в процессе определить легитимность и роль пользователя / компонента, который запрашивает доступ и взаимодействие с системой. Должны быть доступны журналы проверки подлинности и, где это применимо, генерированы отчеты об исключениях. Процесс аутентификации должен быть централизованным
5. Авторизация (контроль доступа): как только пользователь будет подтвержден как легитимный, приложение сможет проверить, к каким ресурсам пользователю будет предоставлен доступ. Авторизация - это право или разрешающая способность, предоставляемая авторизованному объекту для доступа к системному ресурсу. Система допускает управление доступом на основе ролей (RBAC). Роли определяются как набор разрешений. Разрешения будут сгруппированы на основе функциональных ролей. Система обеспечит контроль доступа на основе различных критериев, таких как профиль пользователя, местоположение и отделы. Система обеспечит безопасность на уровне данных, при которой пользователи будут иметь доступ только к данным, для которых они были авторизованы. Система должна иметь возможность применять политику на основе ресурсов (данные, URL, веб-страница и т.д.) И профиля / роли пользователя. В системе должно быть предусмотрено, что системный администратор может настраивать политику безопасности на основе бизнес-требований. или случайным образом. Он также информирует о любом несанкционированном изменении данных неавторизованными пользователями во время передачи или хранения. Система обеспечит безопасность и целостность на сеансовом уровне. Как внутренние, так и внешние пользователи должны иметь целостность на уровне сеанса, чтобы гарантировать, что содержимое информации не может быть изменено при передаче. Например, пользователям следует выдавать уникальный идентификационный номер сеанса, когда
6. Целостность: Целостность данных гарантирует, что данные не были изменены, уничтожены или потеряны несанкционированным образом

- они делают свой первый запрос при входе в систему. IP-адрес клиента также должен быть записан и связан с идентификатором сеанса и использоваться для проверки целостности любых запросов.
7. Сквозная целостность: Пользователи (внутренние и внешние) смогут обмениваться документами / данными таким образом, что в случае изменения документов / данных во время передачи это будет очевидно для пользователей. Конфиденциальность требует, чтобы информация не была доступна или раскрыта никаким неуполномоченным физическим лицам, организациям или процессам. Между всеми компонентами приложения и любыми компонентами приложения с интерфейсом должны быть установлены безопасные соединения. Данные, передаваемые между компонентами, будут конфиденциальными. Следовательно, любые передаваемые данные должны быть защищены путем установления безопасных соединений, обеспечивающих целостность данных и конфиденциальность. Связь между различными компонентами, составляющими приложение, должна быть безопасной. Все коммуникации между компонентами должны быть аутентифицированы, авторизованы и использовать шифрование. Вся коммуникационная активность должна проверяться и отслеживаться с помощью набора управленческих отчетов. Связь между администраторами и компонентами системы должна быть безопасной. Опять же, вся коммуникационная активность администраторов должна проверяться и отслеживаться с помощью набора отчетов.
8. Аудит: Результаты аудита предъявлены на/будет подобранной основе в результате выполнения требований аудита безопасности включает распознавание, запись, хранение и анализ информации, относящейся к действиям, имеющим отношение к безопасности. Полученные в результате записи аудита могут быть изучены, чтобы определить, какие действия, связанные с безопасностью, имели место и кто (какой пользователь / приложение) несет за них ответственность. Требования к аудиту безопасности определяют функциональные аспекты генерации журналов, такие как просмотр, архивирование и хранение, которые обеспечивают целостность аудита. Функциональные требования подразделяются на три основные категории,

Генерация данных аудита безопасности

Проверка аудита

Хранение событий аудита

9. Неотказуемость: Неотказуемость с подтверждением происхождения предоставляет получателю данных доказательства того, что подтверждает происхождение данных и, таким образом, защищает получателя от попытки отправителя ложно отказать в отправке данных. Система позволит:

Неотказуемость источника: конкретному департаменту может потребоваться долгосрочная привязка.

доказательство того, что запрос исходил от пользователя, на случай, если пользователь позже откажется от отправки информации.

Неотказуемость получения: это позволяет департаменту доказать, что пользователь получил ответ.

10. Администрирование: Администраторам приложений будут предоставлены простые в использовании функции администрирования.

Для поддерживать идентификацию пользователя	аутентификация атрибутов	и авторизация	Информация.
Административные функции будут доступны администраторам через единую точку входа и надлежащую авторизацию.			

11. Оповещение и уведомления: Механизм оповещения и уведомления отвечает за повышение безопасности

оповещения о событиях, влияющих на безопасность приложения, на основе уведомлений о событиях из системы. Оповещения должны выдаваться как для предопределенных, так и для пользовательских событий. Система оповещения и уведомления должна быть способна классифицировать события по степени серьезности и уведомлять соответствующее лицо подходящими средствами, такими как электронная почта, SMS или консоль, вместе с соответствующими данными, облегчающими дальнейшие действия. Требования к оповещению и уведомлению следующие::

Должен иметь возможность обнаруживать события, информировать заинтересованные приложения о возникновении определенного события и уведомлять заинтересованные стороны. Событиями являются нарушение политик безопасности, отказ в обслуживании, сбой в работе системы и сбой структуры / требований безопасности. Настройка и управление оповещениями, политиками и конфигурациями уведомлений должны быть осуществляться через интерфейс управления безопасностью.

12. Политика безопасности: политика ИТ-безопасности должна быть разработана для обеспечения информационной безопасности, защиты данных и Безопасности приложений.
13. Сканирование приложений: Все приложения должны пройти процесс сканирования кода и тестирования на проникновение перед развертыванием в рабочей среде.
14. Проверка конфигурации: все программное и аппаратное обеспечение установлено с настройкой по умолчанию. Это может привести к недостаточно защищен для производственной среды. Изменение некоторых свойств или функций может значительно снизить уязвимость сетей или приложений для злоумышленника.

### 7.3.5 Компоненты дорожной карты архитектуры безопасности

#### Этап А

1. Регистрация: Единая централизованная регистрация для всего приложения
2. Федеративная аутентификация: Система должна иметь возможность использовать также схему централизованной аутентификации как и аутентификацию на основе приложения
3. Единая точка доступа: единая точка входа для всего приложения
4. Идентификация: должен быть уникальный идентификатор для всех пользователей и приложения
5. Сканирование приложений: Все приложения должны быть проверены на наличие какой-либо уязвимости.
6. Повышение надежности конфигурации: Все приложения и аппаратные средства должны быть изменены, чтобы гарантировать, что значение по умолчанию свойство не создает никакого риска для окружающей среды.

#### Этап В

1. Централизованная аутентификация: Приложение должно использовать механизм централизованной аутентификации.

Для аутентификации не следует использовать локальный пользовательский репозиторий

Целостность: Все приложения должны иметь безопасность сессионного уровня

2. Авторизация

на основе политики: Авторизацией следует управлять из центрального пользовательского репозитория.

4. Сквозная целостность: Все приложения должны использовать безопасность транспортного уровня при взаимодействии с другими

приложением.

5. Аудит: Все приложения должны иметь функцию аудита для отслеживания того, кто выполнял

определенное действие и когда.

6. Отказ от ответственности: Приложение должно быть способно предоставить доказательства происхождения данных и получателя

данных

Политика безопасности: Необходимо разработать политику безопасности информации, данных и приложений

- 7.

#### Фаза С

1. Администрирование: Утилита централизованного администрирования для всех приложений в организации.
2. Оповещение и нотификация: системы для оповещения о событиях, связанных с безопасностью, с определением степени их серьезности и их пересылкой это

Справка: Для подробного описания каждого элемента архитектуры безопасности обратитесь

к GEA Enterprise Architecture continuum и репозиторию архитектуры.

Обратитесь к отчету GEA - Архитектура безопасности в Непале для получения подробной

информации, относящейся к безопасности Архитектура

## Архитектура инфраструктуры 7.4

### 7.4.1 Принципы архитектуры инфраструктуры

Принцип # 1	
Имя	Масштабируемость, доступность, резервное копирование и архивирование
Заявление	<p>Масштабируемость: Выбранные технологические стандарты должны соответствовать изменяющимся и растущим потребностям и предписаниям министерства, а приложения и технологии должны существенно расширяться, чтобы адаптироваться к таким изменениям требований и колебаниям спроса и реагировать на них. Мощности сервера, хранилища и сети должны выдерживать нагрузку пользователей, приложений и данных.</p> <p>Доступность / отказоустойчивость: технологическая инфраструктура не должна иметь единой точки отказа.</p> <p>Архивирование и резервное копирование: система будет располагать данными и источниками, охватывающими несколько лет. Политика и механизм архивирования и резервного копирования должны соответствовать требованиям системы к архивированию и резервному копированию .</p>
Обоснование	Необходимо для поддержки общих требований SLA в отношении масштабируемости, доступности и производительности
Последствия	<p>Системная инфраструктура должна быть спроектирована с учетом требований к отказоустойчивости и обеспечивать, чтобы сбой одного сервера или сетевого канала не приводил к выходу из строя всей системы (хотя, например, производительность может снизиться).</p> <p>Система должна обрабатывать каждый запрос и выдавать ответ. Она должна эффективно обрабатывать ошибки и исключительные ситуации.</p> <p>В случае сбоев потребуется восстановление транзакций и данных. Платформенное решение должно поддерживать эффективное аварийное восстановление Необходимо регулярно отслеживать работоспособность систем. Использование центральной системы, инструмент мониторинга требуется для постоянной оценки работоспособности системы и мониторинга в соответствии с заранее определенным SLA.</p>

### 7.4.2 Базовая архитектура инфраструктуры.

PwC провела опрос, посетив руководителей ИТ-служб и соответствующие департаменты, чтобы получить представление о текущем состоянии ИТ-инфраструктуры в государственных органах. В следующей таблице приводится общее резюме обследования -

Параметры обследования		Непальская полиция	KMC	SC	EC	FCGO	DoR	NTA	МоГА	DoLR M
1	Узел сервера приложений	ДА	НЕТ	ДА	ДА	3 Вечеринка	ДА	ДА	ДА	НЕТ
2	узел сервера управления & контентом создания	3 Вечеринка	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ

Параметры съемки		Полиция Непала	KMC	SC	ЕС	FCGO	DoR	NTA	MoGA	DoLR M
3	Узел сервера каталогов	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ
4	Узел сервера базы данных	ДА	НЕТ	ДА	ДА	3 Вечеринка	ДА	ДА	ДА	НЕТ
5	Узел файлового сервера	ДА	НЕТ	ДА	ДА	ДА	ДА	ДА	ДА	ДА
6	Узел сервера доменных имен	3 Вечеринка	НЕТ	НЕТ	НЕТ	3 Вечеринка	НЕТ	НЕТ	НЕТ	НЕТ
7	Серверный узел брандмауэра	ДА	НЕТ	ДА	ДА	НЕТ	ДА	НЕТ	ДА	НЕТ
8	Общая информация узел рабочей станции	цель	ДА	ДА	ДА	ДА	ДА	ДА	ДА	ДА
9	Промежуточное программное обеспечение/ серверный	интеграция	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ
узел 10	Узел киоска		НЕТ	НЕТ	НЕТ	ДА	НЕТ	НЕТ	НЕТ	НЕТ
11	Главный ретрансляционный узел	3 Вечеринка	НЕТ	ДА	3 Вечеринка	3 Вечеринка	3 Вечеринка	3 Вечеринка	3 Вечеринка	НЕТ
12	Публика Клавиша инфраструктура		НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ
13	услуги Узел сервера безопасности		НЕТ	НЕТ	ДА	НЕТ	ДА	НЕТ	ДА	НЕТ
14	Узел управления системами		НЕТ	НЕТ	НЕТ	ДА	НЕТ	НЕТ	НЕТ	НЕТ
15	Передача голоса по IP-шлюзу		НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ
16	веб-сервер Информационный	узел	-	3 Вечеринка	НЕТ	НЕТ	3 Вечеринка	НЕТ	НЕТ	НЕТ
17	веб-сервер	узел	-	НЕТ	НЕТ	НЕТ	ДА	НЕТ	НЕТ	НЕТ
18	Транзакционный Серверный узел рабочего процесса		НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ	НЕТ
19	Узел балансировки нагрузки		MP	НЕТ	НЕТ	НЕТ	НЕТ	ДА	НЕТ	НЕТ
20	Схема высокоуровневой инфраструктуры для		НЕТ	НЕТ	НЕТ	ДА	НЕТ	НЕТ	НЕТ	НЕТ
21	управления инфраструктурой серверного узла / сети		ДА	ДА	ДА	ДА	ДА	ДА	ДА	ДА

Опрос показал, что, хотя FCGO, MoGA и Верховный суд Непала имеют относительно безопасную среду по сравнению с другими ведомствами, им не хватает инструментов управления ресурсами и их оптимизации. Текущий сценарий разнообразен: инфраструктура в департаментах, таких как муниципалитеты, практически минимальна, и в то же время такие департаменты, как Почтовый департамент и MoGA, обладают значительными возможностями в области информационных технологий и имеют прогрессивную дорожную карту внедрения информационных технологий.

Этот разнообразный спектр ИТ-зрелости требует проведения значительных мероприятий по наращиванию потенциала с точки зрения ИТ осведомленности и предоставления возможностей ИТ, чтобы вывести департаменты на минимальный уровень общей инфраструктуры. Чтобы в общих чертах описать соответствующее текущее состояние ИТ-инфраструктуры, был рассмотрен текущий инфраструктурный ландшафт следующих 3 департаментов с относительно безопасной средой

1. Полиция Непала
2. Почтовый департамент
3. Министерство общего управления

Полиция Непала осуществляет операции с чрезвычайно конфиденциальными и защищенными данными, однако текущего уровня управления ресурсами, сетевой безопасности, управления пользователями и инфраструктуры физической безопасности недостаточно для обеспечения даже базового уровня безопасности. Мы также рекомендуем, чтобы SWAN, который в настоящее время арендуется у NTC, был собственным ресурсом для обработки таких важных данных, имеющих отношение к национальной безопасности.

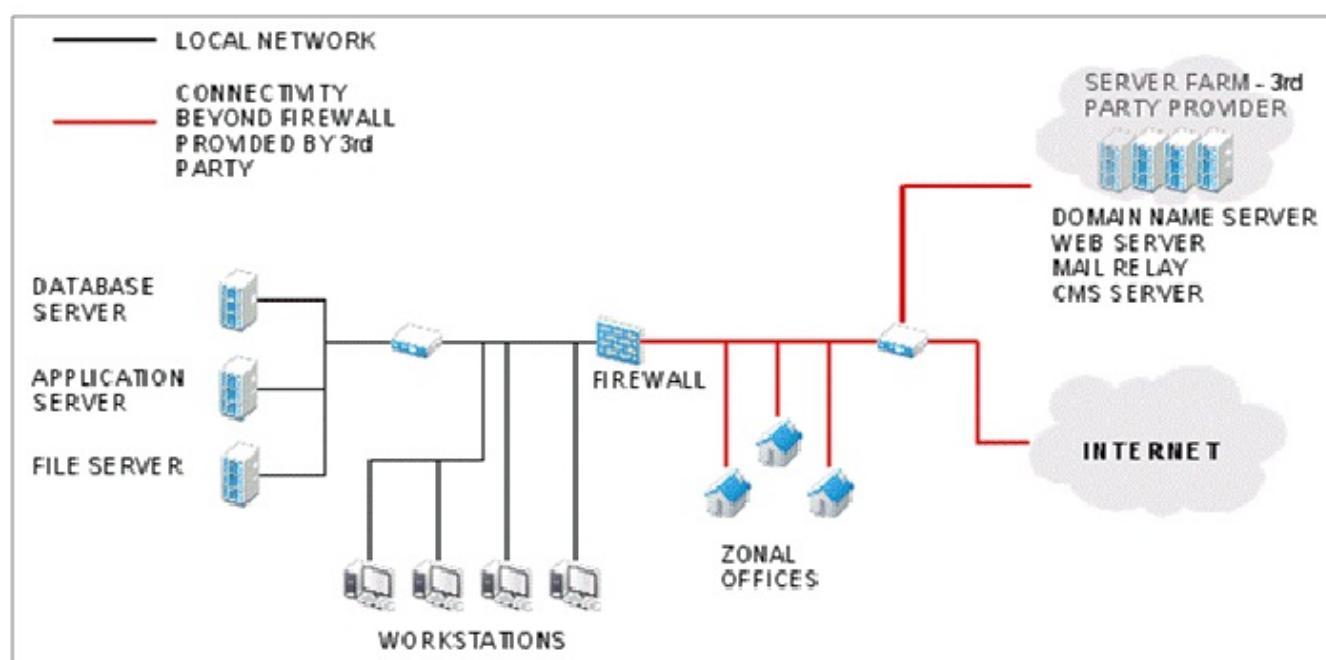
Департамент должностей ограничен с точки зрения управления ресурсами, управления пользователями и физической безопасности. Однако они преуспели во внедрении множества технологий, имеющих отношение к различным операциям, и обладают потенциалом и зрелостью для расширения / интеграции в инфраструктуру общих ресурсов.

Министерство общего управления имеет прочную и надежную связь с другими министерствами и ведомствами в комплексе Сингх Дурбар. Существует дублирование инфраструктуры с Министерством финансов для обеспечения избыточности. Это опять же соответствующие мощности, которые могут быть перенесены в инфраструктуру общих ресурсов.

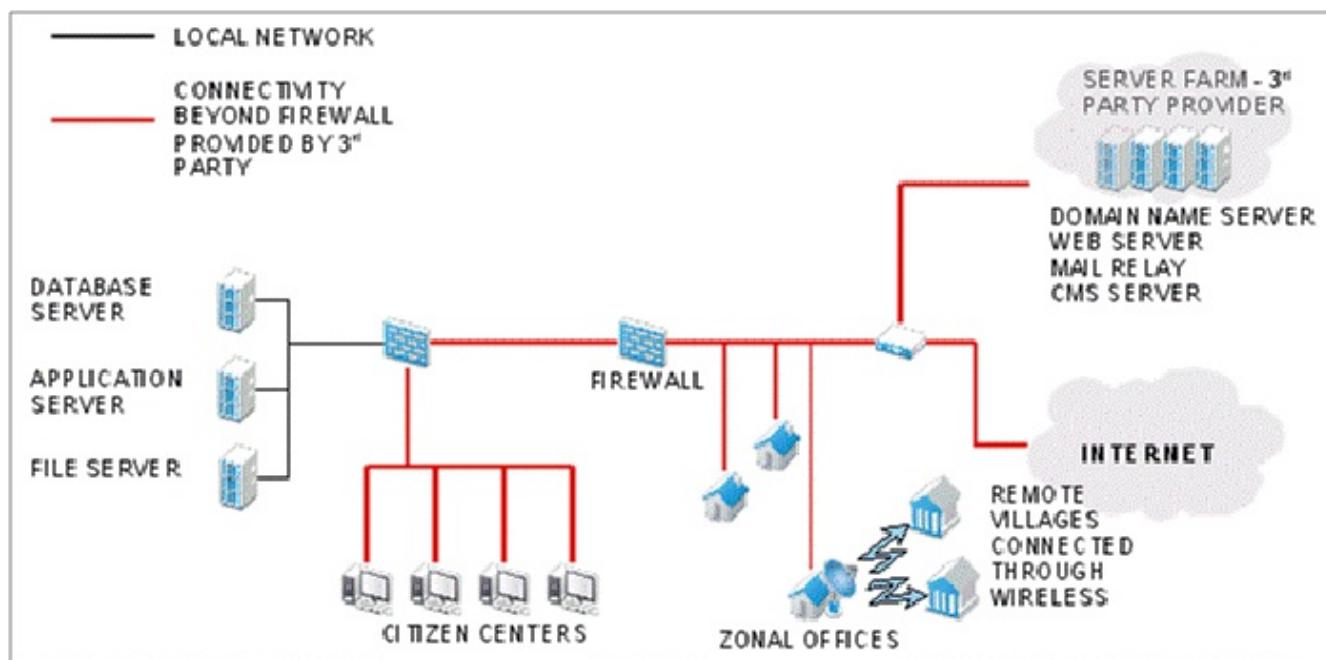
Другие департаменты, такие как Департамент автомобильных дорог и Департамент земельных реформ и управления, имеют операционную инфраструктуру с различными компонентами, однако значительное количество этих компонентов являются "устаревшими" и требуют модернизации. Их ИТ-потенциал также нуждается в расширении с точки зрения инструментов управления и наборов навыков. Таким образом, они становятся идеально подходящими для использования общей инфраструктуры вместо создания индивидуальных мощностей для каждого из этих отделов.

Схема инфраструктуры очень высокого уровня для вышеупомянутых трех типичных департаментов приведена ниже для справки

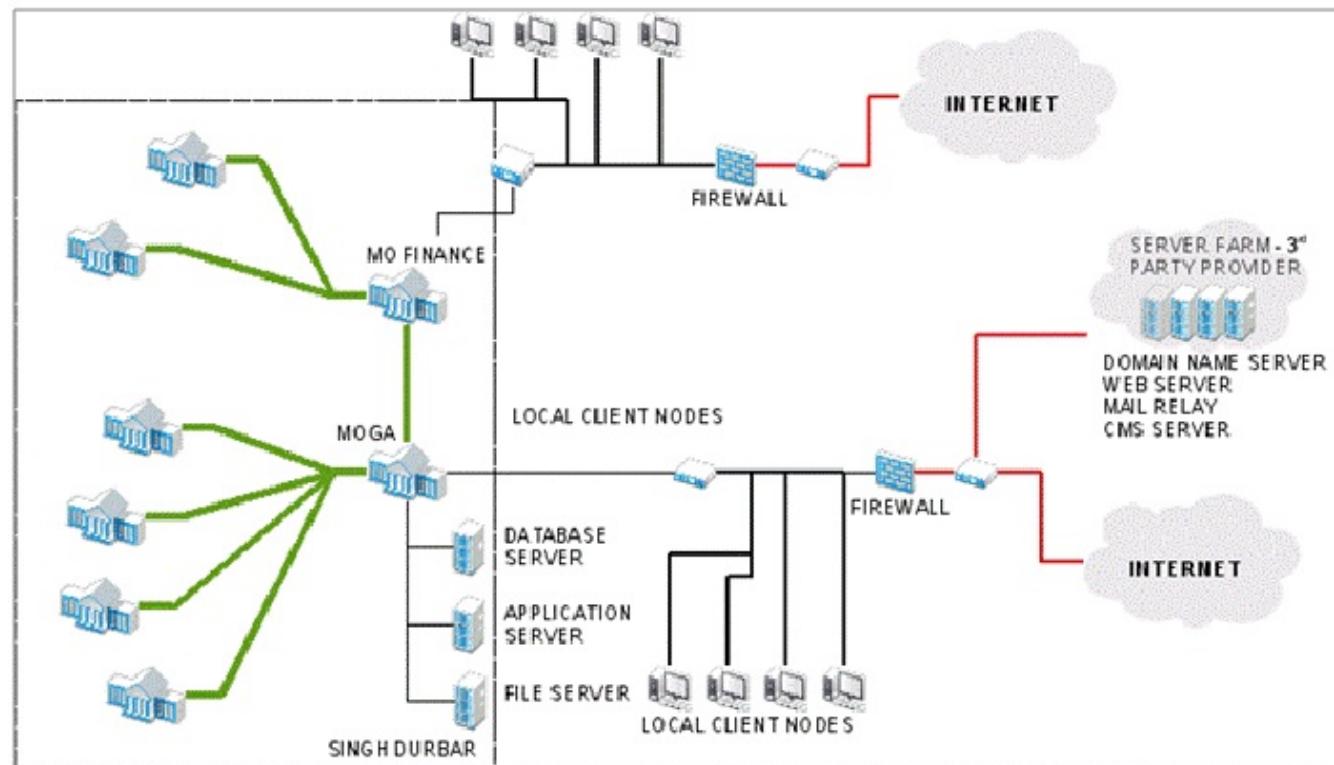
#### Полиция Непала



#### Почтовый департамент



MOGA



#### 7.4.3 Архитектура целевой инфраструктуры

Информационные технологии являются ключевым фактором, способствующим процессу разумного электронного управления, предлагая доступ и предоставление услуг, соответствующих ожиданиям людей:

Горизонтальная и вертикальная интеграция внутри организации необходима для эффективного обмена информацией.

За этим должно последовать разрешение публичного доступа к управлению в различных точках этого горизонтального и вертикального информационного коридора.

Стандартизация и преобразование всех обращений правительства, ориентированных на граждан, в электронную форму для интерактивного общественного использования является последним шагом в процессе электронного управления.

Для практической реализации цели электронного управления следует планировать развертывание ИТ-инфраструктуры по всей стране с двух точек зрения:

#### **Общая и защищенная сеть и**

#### **Услуги общего центра обработки данных**

Чтобы помочь правительству Непала улучшить совместное использование ИТ-инфраструктуры между ведомствами, в архитектуре технологии / инфраструктуры предлагается набор передовых практик и конструктивных соображений, которые касаются:

Общей инфраструктуры

Услуг общего центра обработки данных

Общие службы безопасности

Общие службы управления инфраструктурой (ввод сети и данных)

#### **Общие и защищенные сети**

Сегодня правительства все чаще обращаются к гибкости IP-сетей для предоставления конвергентных услуг передачи голоса, видео и данных. Конвергентная сеть с особым упором на "открытые стандарты" (для внутриорганизационного обмена и за его пределами). Это дает двойное преимущество снижения затрат и повышения эффективности.

Затраты снижаются, поскольку несколько агентств могут использовать общие инвестиции. Кроме того, поставщик услуг может максимально эффективно использовать ресурсы общей сети и центра обработки данных, превращая выделенные ресурсы, назначенные каждому приложению в каждой группе, в общий пул ресурсов, который может динамически распределяться в зависимости от потребностей приложений и бизнеса.

Эффективность повышается за счет того, что единой общей инфраструктурой легче управлять и перенастраивать в соответствии с меняющимися потребностями правительства и субъектов, которым она служит. Используя общую инфраструктуру, агентства могут легко обмениваться приложениями и информацией на основе политики и спроса на приложения, позволяя создавать новые приложения на основе потребностей участников, а не государственной иерархии.

Учитывая текущие и будущие тенденции, основными техническими требованиями для полной архитектуры общей инфраструктуры являются:

Удаленный доступ из филиалов или дома и возможность устанавливать VPN-соединение с сетью во время поездок

Логическая изоляция трафика от соответствующих пользователей

Возможности аутентификации и ведения журнала

Учет, фильтрация, проверка содержимого и безопасность

Беспроводная поддержка как проводного, так и беспроводного доступа

#### **Службы общего центра обработки данных**

Центры обработки данных развиваются, и государственные учреждения, специализирующиеся на архитектуре общей инфраструктуры, могут извлечь выгоду из этой эволюции. В центрах обработки данных находится множество критически важных активов для государственных учреждений, включая системы хранения данных, приложения и серверы, которые поддерживают повседневную работу. Традиционно в этих центрах обработки данных размещались мэйнфреймовые компьютеры, затем клиентские и серверные системы. Сегодня центры обработки данных стали чрезмерно сложными, порой недостаточно используемыми и истощающими физические ресурсы, такие как тепло, пространство и электропитание. Однако эти расширения

также предусмотрены масштабируемость, надежность и доступность. По мере разработки архитектуры общей инфраструктуры для центров обработки данных эти недостатки должны быть устранены при сохранении положительных критических характеристик.

Стоимость является наиболее важным фактором консолидации центров обработки данных, поскольку по мере расширения центров обработки данных для удовлетворения требований агентства, когда появляется все больше серверов, приложений и устройств хранения данных, их поддержка и обслуживание становятся все более дорогостоящими. Затраты включают в себя недвижимость, необходимую для хранения оборудования, часть которого может работать лишь на малой мощности, мощность для запуска оборудования и техническое обслуживание устройств. Следовательно, хотя капитальные затраты оказываются первоначальное финансовое воздействие, периодические операционные расходы создают огромную финансовую нагрузку для государственных учреждений, особенно когда многие государственные учреждения содержат свои собственные центры обработки данных с низкой пропускной способностью и неэффективностью.

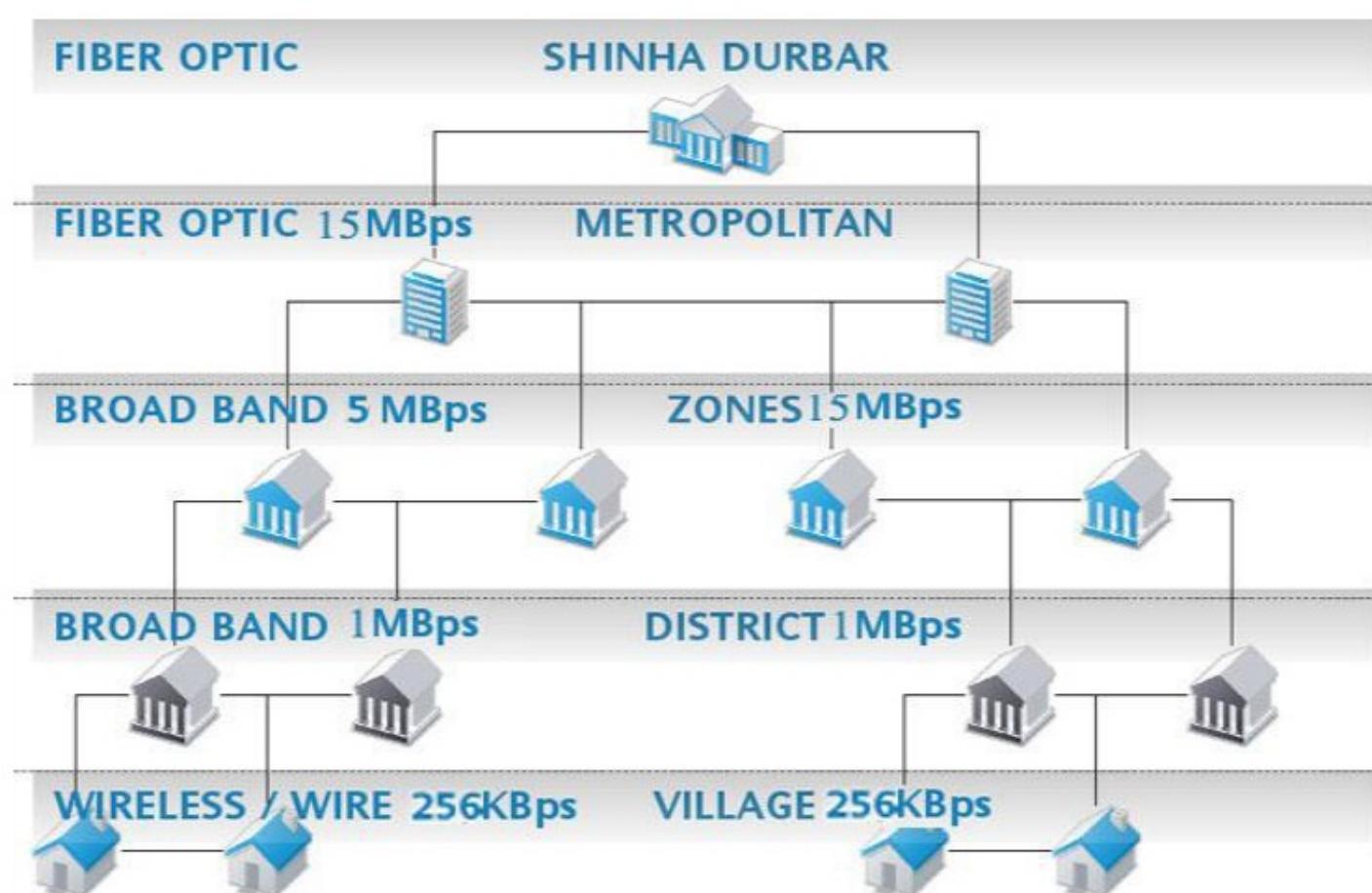
#### **Общая инфраструктура - общие соображения по проектированию**

Правительству Непала следует создать современную сетевую инфраструктуру в рамках проекта Nepal Wide Area Network Project (NWAN) со следующими целями:

1. создать надежный горизонтальный и вертикальный коммуникационный коридор для государственной администрации, чтобы сделать правительство более продуктивным и совместимым с электронными транзакциями; 2. добиться приверженности электронному управлению и приблизить управление к обществу; 3. укрепить потенциал реагирования на стихийные бедствия.;

Мы рекомендуем настроить эту государственную инфраструктуру сети ИКТ (Nepal Wide Area Network - NWAN) для обеспечения:

1. Передача голоса, Видео и Данных - все услуги по IP,
2. объедините 14 зон и 75 районных офисов в сеть, способную обрабатывать большие объемы и высокоскоростные данные и проводить видеоконференции 3. впоследствии подключайте стратегически выбранные деревни, насчитывающие более 1000 человек 4. Одна надежная сеть кампуса в Сингх Дурбаре (SDAN), подключенная к NWAN, обеспечивает подключение доступ вплоть до районного уровня для всех сотрудников секретариата и наоборот,
5. Подключение спутника к NWAN Hub для обеспечения присутствия всех служб сети Omnip в информации о штате / стране на уровне деревни через терминал VSAT или местной беспроводной связи, если позволяет инфраструктура.



Для подключения на очень высоком уровне мы рекомендуем следующее:

Сингх Дурбар - Безопасная волоконно-оптическая связь между всеми министерствами в Сингх Дурбаре, имеющая

Сеть с пропускной способностью 15 Мбит / с с резервированием . Катманду

- Все департаменты в пределах Катманду должны быть подключены к Сингх Дурбар по оптоволокну

подключение к сети с пропускной способностью 5 Мбит / с с резервированием Зоны

- Зональные офисы должны быть подключены к Катманду и Сингх Дурбару широкополосной связью со скоростью 5 Мбит / с

офисы с пропускной способностью сети 15 Мбит / с с резервированием

Районы - Районные офисы должны быть подключены к офисам zonal и Singh Durbar как минимум с 1

Сеть с пропускной способностью Мбит / с с резервированием .

деревни - деревни могут быть подключены к районным офисам с помощью беспроводной или другой связи сеть с пропускной способностью не менее 256 Кбит / с с резервированием.

#### Архитектура и топология сети NWAN:

Мы рекомендуем, чтобы NWAN был основан на конструкции "стуница и спицы" с 3 уровнями:

Уровень 1 - NITC в Сингха Дурбаре, офисы секретариата в Сингха Дурбаре и метрополитене, а также офисы секретариата в Катманду, где должны быть расположены высшие государственные

должности, соединенные горизонтально через сеть кампуса Дурбара (DCAN). Районные центры

(DCS) будут соединены по вертикали с этой сетью кампусов. 2. Уровень

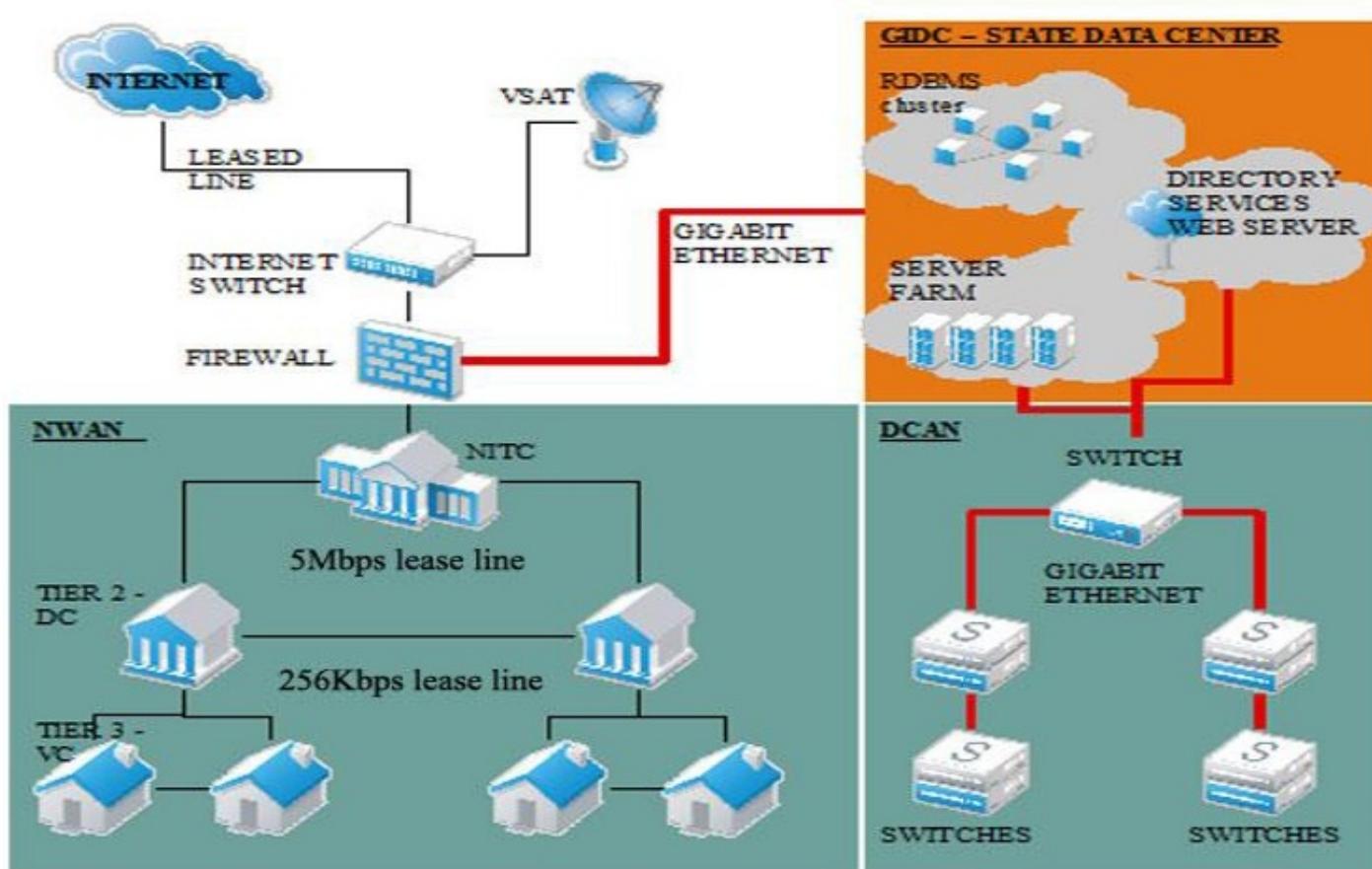
2 - Районные и зональные офисы различных секретариатов будут соединены по горизонтали с

Районный центр (округ Колумбия).

3. Уровень 3 - Местные сельские офисы, где это применимо, будут подключены горизонтально к центру деревни.

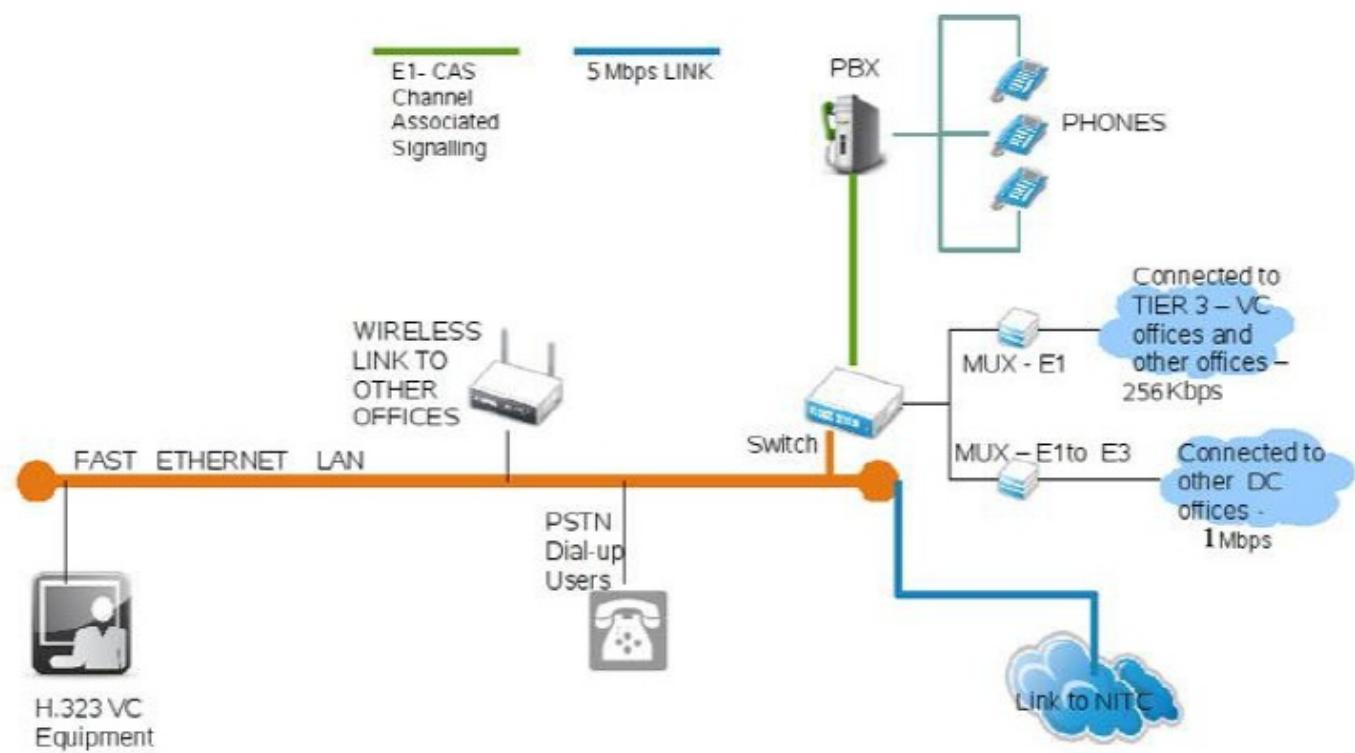
(VC), который, в свою очередь, был бы вертикально соединен с районным центром (DC).

NITC является сетевым центром. Сеть кампуса Дурбара (DCAN) интегрируется с NWAN в NITC (как показано на рисунке ниже).



Рекомендуемая конструкция для NWAN - это общая IP-сеть. В таком сценарии данные, голос и видео передаются по сети в виде IP-пакетов с полной конвергенцией.

#### Уровень 1: Сеть центров NITC NWAN



Как показано на приведенной выше схеме, сеть в центре NITC NWAN состоит из всех компонентов

центрального узла-хаба.

Существующие подключения к данным (по оценкам, 5000 - 10000) в DCAN должны быть подключены к NWAN. Все правительственные учреждения и каждый из (по оценкам, от 5000 до 10000) пользователей Секретариата в столице должны иметь возможность проводить видеоконференции (VC) с любым одним или всеми главными блоками управления (MCU) в сети в любом месте штата.

#### **Функция мобильности, введенная в GSWAN:**

Расширенная станция VSAT с-диапазона (необходимо получить второе мнение по этой рекомендации) должна быть подключена к локальной сети NITC, чтобы обеспечить соединение NWAN с портативным VSAT mobile, работающим в удаленном удаленном местоположении. Это позволит предоставлять услуги глобальной сети в местах, где полностью отключена связь . События, происходящие в удаленных точках, покрываются и подключаются к NWAN через портативный терминал VSAT. Это даст государственной администрации огромную гибкость в обращении к населению в удаленных районах во время любой чрезвычайной ситуации.

#### **Беспроводная сеть для других важных офисов, недоступных для подключения по кабелю:**

Можно ввести в эксплуатацию беспроводную локальную сеть для подключения к DCAN, если они не подключены к магистрали Ethernet кампусной сети.

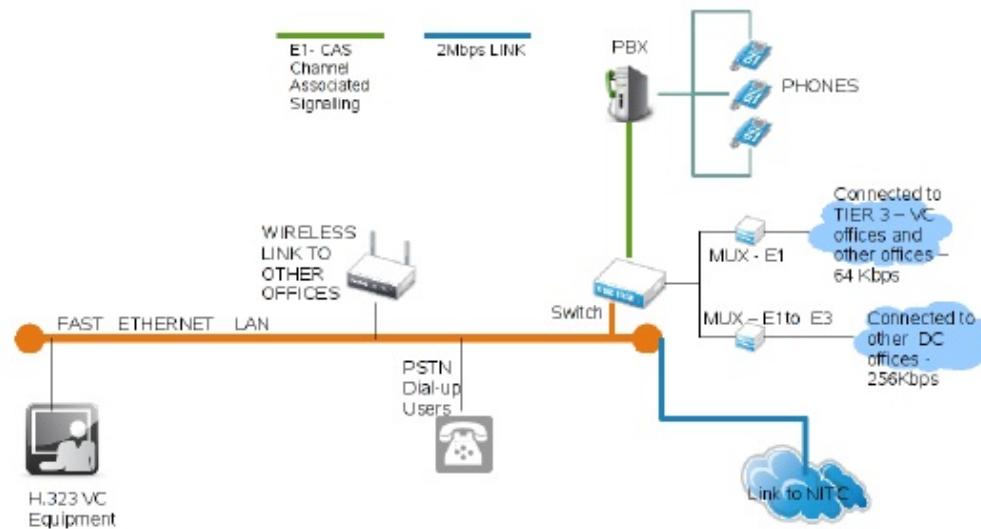
#### **Ферма серверов:**

В ферме серверов государственного центра обработки данных в GIDC можно ввести в эксплуатацию несколько серверов. Всеми распространенными ИТ-сервисами, а именно Интернетом, веб-хостингом и обслуживанием, хранением и поддержкой базы данных, почтовыми службами и т.д., можно управлять из сервисного центра серверной фермы, связанного с NWAN и DCAN.

#### **Уровень 2 - Районный центр - Типовая архитектура**

Узел NWAN в Окружном центре должен иметь в наличии все средства передачи голоса, видео и данных.

Районы в каждой зоне должны иметь окружной центр NWAN (DC) и быть соединены горизонтально в офисе зоны в дополнение ко всем деревенским узлам NWAN (VC), находящимся под его юрисдикцией. Офисы, уполномоченные



правительство должно иметь возможность входить в Сеть через удаленный доступ. Сервер удаленного доступа (RAS) на

каждом DC должен иметь 10 коммутируемых линий ТСОП, обеспечивающих доступ тем, кто не подключен напрямую к NWAN.

#### **Службы общего центра обработки данных - общие соображения по проектированию**

В рамках подхода, основанного на архитектуре общего центра обработки данных, центр передового опыта предоставляет каждому агентству единый набор услуг центра обработки данных, которые являются технологически современными и гораздо более экономичными.

Для достижения этой цели общий центр обработки данных следующего поколения должен соответствовать следующим требованиям:

**Масштабируемость, доступность и надежность-** Объединение инфраструктуры в общую среду LAN / WAN приводит к созданию каналов Ethernet с более высокой пропускной способностью 10 Гигабит в сети доступа и агрегирования при сохранении конструкции высокой доступности, гарантирующей, что центры обработки данных всегда доступны.

**Безопасность-** все более важным фактором при проектировании сетей является безопасность, требующая наличия как продуктов, так и набора передовых разработок в области безопасности для обеспечения того, чтобы критически важные активы центров обработки данных могли противостоять известным угрозам "нулевого дня".

**Сегментация-** Консолидация центров обработки данных обеспечивает надежное распределение ресурсов и полное использование активов, тем самым максимально расширяя возможности оборудования. В общей среде сегментация позволяет нескольким агентствам совместно использовать активы, которые разделены в соответствии с требованиями каждого агентства.

**Виртуализация.-**благодаря пропускной способности глобальной сети несколько узлов для центров обработки данных и агентств теперь могут виртуализировать больше ресурсов в центре обработки данных и разгрузить управление оборудованием на месте. Эти ресурсы могут размещаться в нескольких центрах обработки данных для обеспечения большей живучести в случае непредвиденных обстоятельств, которые могут привести к выходу из строя определенного сайта.

**Разведывательные данные-**Разные отделы предъявляют разные требования к приложениям, что может привести к перегрузке центра обработки данных . Интеллектуальные блочные сервисы обеспечивают ускорение приложений, повышенную безопасность приложений и методы упрощения инфраструктуры приложений для обеспечения более быстрого развертывания новых серверов приложений.

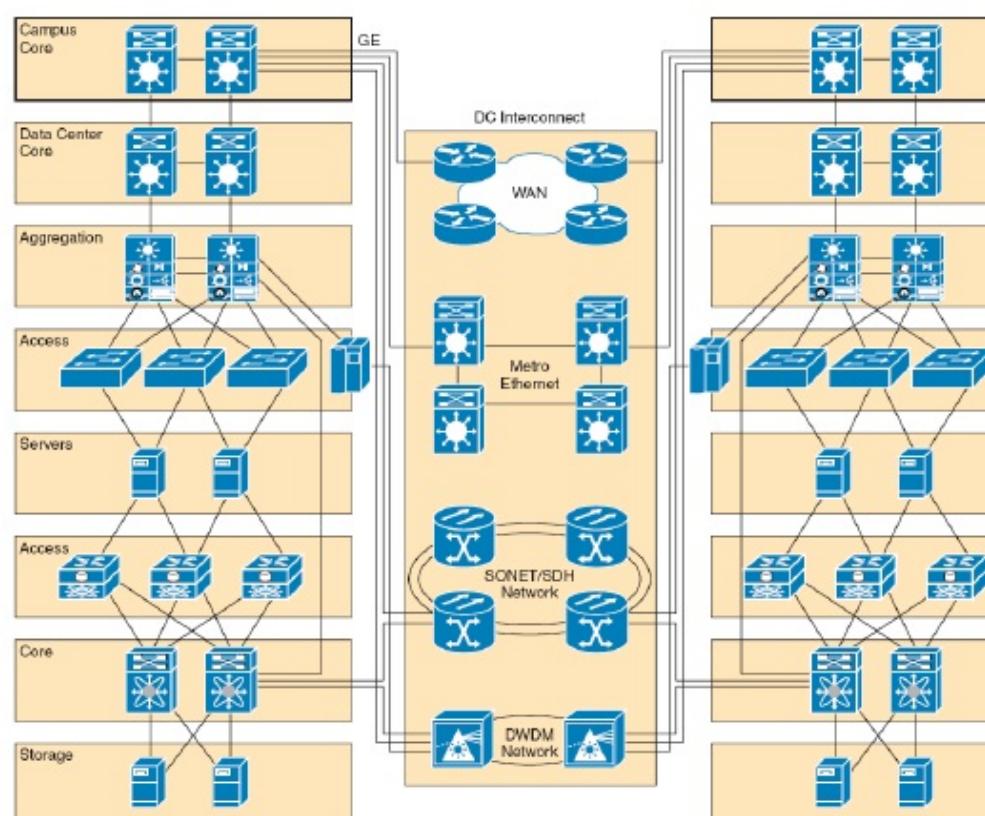
**Управляемость-**этот подход центра передового опыта упрощает управление центром обработки данных. Благодаря сегментации инфраструктуры и виртуализации в комплекте с инструментами управления от Cisco и

партнеры, общая архитектура центра обработки данных значительно снижает накладные расходы агентства и упрощает операции. Архитектура общей инфраструктуры, отвечающая этим требованиям, помогает снизить совокупную стоимость владения , позволяя центру обработки данных эффективно удовлетворять потребности множества агентств. Это может помочь устраниć любые нормативные или политические препятствия, с которыми могут столкнуться усилия по консолидации. Наконец, достигнутая эффективность не только снижает затраты, но и позволяет государственным учреждениям более эффективно разрабатывать инструменты для обслуживания своих клиентов.

### Архитектура центра обработки данных - подход

Архитектура общего центра обработки данных в рамках подхода к общей инфраструктуре может быть очень сложной.

Компоненты центра обработки данных здесь упрощены для изучения конкретных требований хорошо спроектированного общего центра обработки данных для нескольких агентств.



Строительные блоки.:

Сетевые области - ядро, агрегация, доступ и DC interconnect

Структура сети-уровни 2 и 3, высокая доступность и кластеризация

Виртуализация и сегментация сети

Сетевой интеллект

Сетевая безопасность

Структура серверов

Структура SAN

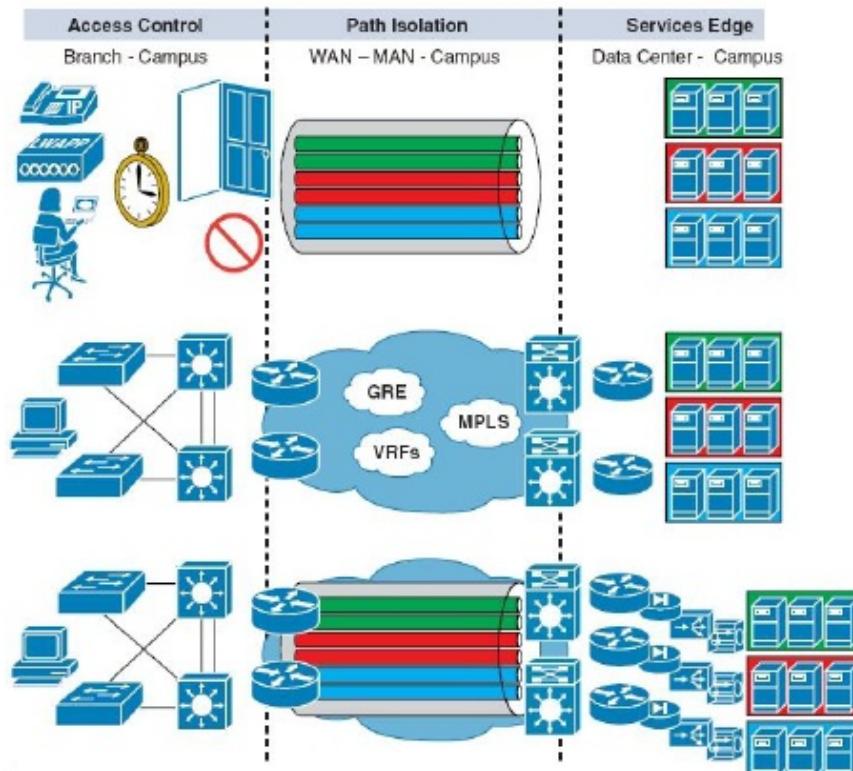
Архитектурная структура разделена на три функциональные области, каждая из которых соответствует одной из целей:

Контроль доступа

Изоляция путей

Граница служб

1. Идентификация и аутентификация клиента (пользователя, устройства, приложения), пытающегося получить доступ к сети, Изолировать в сегменте, предоставить \_controlled\_access или запретить доступ
- Сопоставьте клиентскую VLAN с транспортной 4. технологии
5. Транспортируйте клиентский трафик по изолированному пути.
- Завершите изолированный путь @ граница назначения
7. Сопоставьте изолированный путь к локальной сети назначения
- Применить политику на входе в VLAN 8. пункт
9. Изолировать приложение среды



#### 7.4.4 Анализ пробелов

Ниже приведены пробелы, выявленные между базовой и целевой архитектурами. Список выявленных возможностей таков

1. Безопасность

Общие службы безопасности

Общая инфраструктура безопасности

Сетевая безопасность в защищенном сегменте

2. Государственная Глобальная сеть

3. Государственный центр обработки данных

Эксплуатация центра обработки данных и системное управление - ITIL

Соображения безопасности Центра обработки данных

Структура безопасности центра обработки данных

Автоматизация центра обработки данных

## 4. База данных управления конфигурацией

## 5. Управление инфраструктурой

Справка: Для получения подробного описания каждого элемента архитектуры инфраструктуры обратитесь к GEA Континуум архитектуры предприятия и репозиторий архитектуры. Обратитесь к отчету "Непальская GEA -Архитектура инфраструктуры" для получения подробной информации, относящейся к архитектуре инфраструктуры

### 7.4.5 Компоненты дорожной карты архитектуры инфраструктуры

#### 7.4.5.1 Дорожная карта - внедрение общей сети

Архитектура общей инфраструктуры может принести множество преимуществ государственным учреждениям, стремящимся удовлетворить многие современные требования к ИТ и совместной работе.

Государственные программы и технические архитектуры PWC, основанные на платформе SONA, интегрируют сетевые инфраструктурные сервисы, составляющие сервисы и бизнес-приложения внутри агентств и между ними.

Наличие поэтапной дорожной карты позволяет успешно перейти от текущей инфраструктуры к архитектуре, поддерживаемой центром передового опыта, который обеспечивает совместное использование инфраструктуры и услуг несколькими агентствами. На каждом этапе дорожной карты внедряются новые технологии для создания общей инфраструктуры, которая позволяет агентствам обмениваться услугами через центр передового опыта. У каждого агентства могут быть разные потребности, требующие более быстрого выполнения некоторых задач, но в приведенной ниже таблице показан переход к модели общей инфраструктуры, разбитый на логические этапы.

ТЕХНОЛОГИЯ	Общий / Выделенный для разных агентств	Описание
1. Разделение по времени Мультиплексирование (TDM)	Выделенный канал	Текущее состояние сети, которое обычно характеризуется изолированными технологиями TDM, такими как УАТС для передачи голоса и Frame Relay / ATM для передачи данных.
2. IP-сеть	Выделенная	Первый шаг в переходе от технологий TDM к инфраструктуре с поддержкой IP, которая закладывает основы для того, чтобы произошла трансформация. IP-сеть должна быть построена с учетом сетевых характеристик для поддержки QoS, высокой доступности и т.д. Обеспечения
3. IP-коммуникации	Выделенные	"унифицированных коммуникаций", голосовой почты, конференц-связи, мультимедийной связи и дополнительной мобильности. Включите централизованный контактный центр для обеспечения интеллектуальной
4. IP-контактный центр	Выделенный	маршрутизации и обработки вызовов для поддержки клиентского контакт-центра с поддержкой IP. Обеспечьте каждому сайту безопасность, необходимую для поддержания бизнеса, с помощью таких
5. Самозащита Сетевая безопасность	Выделенный	возможностей, как брандмауэры с отслеживанием состояния, защита и предотвращение вторжений, фильтрация URL-адресов и доверие.

ТЕХНОЛОГИЯ	Общий / Выделенный для разных агентств	Описание
		и идентификация.
		Межсайтовая VPN с IPsec для шифрования, когда требуется.
		DCN для внеполосного управления.
6.	Интеллектуальная маршрутизация	Выделенный сервис  QoS для обеспечения взаимодействия от объекта к объекту, равного взаимодействию в одном месте, что является ключевой основой для поддержки дифференцированных услуг.  Иерархическая, сквозная сеть.
7.	Мобильность	Выделенный персонал  Включите мобильную IP-связь для поддержки мобильной рабочей силы.
8.	Центр обработки данных	Выделенный  Консолидация центра обработки данных в централизованную среду обеспечивается с помощью структуры IP-сетей, которая поддерживает сетевую ДНК для преобразования архитектуры центра обработки данных.
9.	Интеллектуальная маршрутизация	Общий доступ  Включите виртуализацию и сегментацию интеллектуального уровня маршрутизации для поддержки общих ресурсов инфраструктуры в нескольких агентствах.
10.	Самозащита Сетевая безопасность	Общий доступ  Виртуализируйте функции безопасности, такие как брандмауэр, в сети для поддержки нескольких агентств.
11.	Центр обработки данных	Выделенный  Включите консолидацию центра обработки данных с сервером и хранилищем fabric.
12.	IP-коммуникации	Общие  Виртуализируйте IP-коммуникации с помощью централизованной сети, поддерживающей голосовую почту, конференц-связь и другие мультимедийные коммуникации для нескольких агентств.
13.	IP-Контактный Центр	Общий доступ  Виртуализируйте IP-контактный центр для нескольких агентств.
14.	Центр обработки данных	Общий доступ  Консолидируйте функции центра обработки данных для нескольких агентств и внедрите ускорение приложений и балансировку нагрузки.
15.	Центр обработки данных	Общий доступ  Виртуализируйте функции центров обработки данных в нескольких агентствах и внедрите оптимизацию / перевод протоколов приложений.

#### Дорожная карта 7.4.5.2 - Консолидация центров обработки данных

##### Этап 1 - Базовый уровень инвентаризации ИТ-активов (включая предварительную оценку и быстрые выигрыши)

Оценка будет включать такие детали, как местоположение объекта, то, как и кем используется центр обработки данных,  
является ли объект автономным или совмещенным с другими видами деятельности, площадь объекта, сведения о юридическом владении,

измерение потребления энергии и текущих затрат. От тех, кто проводит оценку, потребуется

Составить реестр HW. Активы SW по центрам обработки данных

Фиксируйте базовые показатели использования и энергопотребления для каждого центра обработки данных

Определите быстрые выгоды, включая конкретные результаты.

Создайте инвентаризацию ИТ-активов для базового уровня и быстрых выгод.

## **Этап 2 - Сопоставление приложений.**

Необходимо приложить усилия для расширения текущего реестра до уровня, на котором администраторы могут сопоставлять приложения:

С серверами

С конкретными базами данных и платформами

С конкретными зависимостями приложений

С конкретными сведениями о безопасности приложений

С подробной информацией об использовании приложений и соглашениях об уровне обслуживания (SLA)

С информацией об архитектуре сегмента

## **Этап 3 - Анализ и стратегические решения**

Выполните оценку энергопотребления и затрат для возможных различных подходов

Определите риски, альтернативы, допущения о стоимости и бизнес-выгоды

Принимайте стратегические решения об инвестициях в технологии и консолидацию

*Конкретные результаты:*

Анализ консолидации и стратегические инвестиционные решения по стандартным платформам и сервисам

## **Этап 4 - Разработка концепции консолидации и план перехода**

Альтернатива консолидации для проектирования и тестирования

Разработка плана перехода для оптимизации энергопотребления и консолидации центра обработки данных

Создание плана проекта и полной структуры распределения работ для плана перехода

*Конкретные результаты:*

Дизайн консолидации и план перехода

## **Этап 5 - Консолидация и оптимизация выполнения**

Выполнение планов виртуализации, консолидации и миграции

Выполнение планов оптимизации энергопотребления

измерение показателей использования и экономии затрат и отчет о них

Конкретных результатов:

Консолидация и проведение плюс отчеты

#### **Этап 6 - Постоянная Поддержка Оптимизации**

На основе уроков *узнала от предыдущей работы, продолжения использования энергии, оптимизации и консолидации*

Удельная результатов:

Текущие полугодовые отчеты метрики

Продолжать постоянный мониторинг и сообщать о показателях использования и экономии средств.

#### **Конечная цель**

Одна из вероятных конечных целей, если масштабные оценки будут слишком медленными, - расширение государственных центров обработки данных за счет сосредоточения внимания на корпоративных архитектурах, которые будут поддерживать больше облачных ИТ-сервисов

## 7.5 NeGIF - Обзор

**NeGIF** обеспечивает основу для обмена, совместной работы и интеграции информационных и организационных процессов путем определения минимального набора стандартов ИКТ и технических спецификаций, регулирующих взаимодействие систем, поток информации, а также обмен данными и бизнес-процессы, которые относятся к правительенным министерствам, агентствам и департаментам. Все более широкое использование открытых стандартов для обеспечения такой интероперабельности является ключом к успеху любой платформы NeGIF и выбору правильного набора технических стандартов и политик, подходящих для конкретной среды.

Ключевыми движущими факторами для NeGIF являются следующие

- Совместимость
- Зрелость сервиса
- Доступность поддержки
- Открытость

Этот NeGIF будет служить следующим целям правительства Непала.:

Предоставлять возможность частным системам с открытым исходным кодом в различных государственных информационных системах, как внутри правительства, так и за его пределами, эффективно взаимодействовать; Продвигать и стимулировать принятие открытых стандартов, которые обеспечивают обмен данными между приложениями;

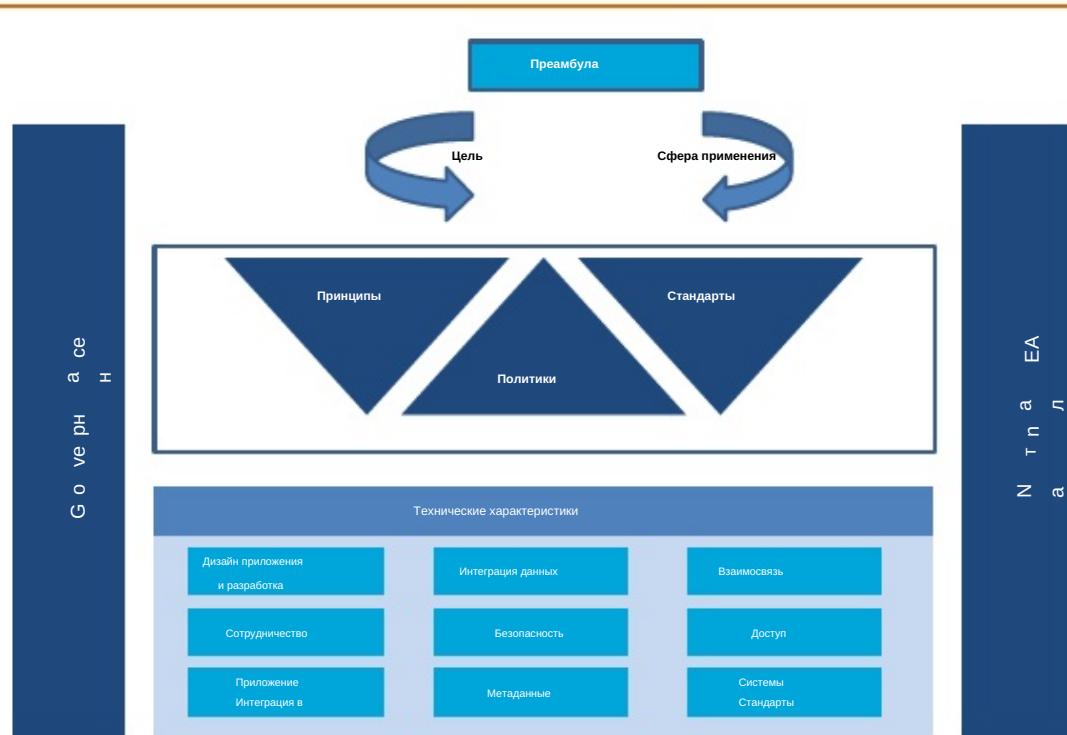
Продвигать независимые от поставщиков и технологически нейтральные внедрения с внедрением открытых стандартов для всех государственных информационных систем; и

Снизить общую стоимость владения государственными информационными системами за счет внедрения открытых стандартов.

Для достижения такого уровня интероперабельности требуется целостный подход, охватывающий различные аспекты стандартов интероперабельности на различных уровнях, таких как интероперабельность бизнес-процессов или организаций, информационная или семантическая интероперабельность и техническая интероперабельность. Ключевые особенности NeGIF -

- XML как основной стандарт взаимодействия с данными
- Все выбранные стандарты поддерживают безопасную вычислительную среду
- Выбранные стандарты могут быть масштабированы в соответствии с изменяющимися требованиями
- Способствуют использованию метаданных
- Использование открытых стандартов, которые широко поддерживаются

Ядром NeGIF является преамбула (охватывающая цель и сферу применения), принципы, политики и стандарты. Управление и архитектура - это аспекты, которые помогут внедрению NeGIF, взаимосвязи, управлению и успеху.



## Пreamble

Пreamble описывает цель и сферу охвата непальского eGIF.

Всеобъемлющей целью NeGIF в Непале должно быть улучшение экономического роста и справедливости путем расширения доступа к информации и ее эффективного использования, тем самым улучшая предоставление услуг в интересах заинтересованных сторон - граждан, предприятий, а также правительства (внутри страны и за рубежом). Целью NeGIF является облегчение обмена данными и информацией между:

<sup>1</sup> Взаимодействие между правительствами (G2G) - внутри правительства Непала, т.е. между правительственными учреждениями и департаментами. Взаимодействие правительства с гражданами (G2C) - между правительством Непала и его гражданами. 2. 3. Взаимодействие правительства с предприятиями (G2B) - Между правительством Непала и предприятиями частного сектора, т.е. поставщиками и подрядчиками правительства.

## Принцип

Обратитесь к ключевым архитектурным принципам взаимодействия.

## Политики

Некоторые из ключевых политик, охватывающих различные аспекты NeGIF, которым необходимо следовать -

### Общая политика

- Все выбранные стандарты должны основываться на цели, сфере применения и принципах NeGIF.
- Везде, где это уместно, следует отдавать предпочтение открытым стандартам перед проприетарными. В случае выбора собственных стандартов принципы NeGIF должны рассматриваться как основное требование Институциональный подход должен быть заменен подходом сервисного центра, тесно связанным со стратегией электронного управления, и соблюдение NeGIF должно быть обязательным для всех государственных министерств, агентств и ведомств.

### Политика в области приложений и технологий

Стандарты должны, насколько это возможно, соответствовать Всемирной паутине для всех общедоступных пользователей. ○  
отраслевые информационные системы.

Разработка приложений или электронных сервисов должна предоставлять услуги пользователям, которые не  
○  
иметь доступ к новейшим технологиям и к тем, кто может не знать об использовании таких  
технологий. Все  
будущие приложения и миграция устаревших приложений должны быть основаны на веб  
(браузере)  
интерфейсах.

При разработке приложений необходимо учитывать особые требования к доступности,  
включая ○  
представление более сложных ресурсов, ориентированных на конкретного  
пользователя. Текущим приложениям, возможно, не требуется немедленное  
соответствие требованиям NeGIF; однако любые новые ○  
информационная система / изменение "апгрейд должны соответствовать требованиям. Данная  
версия NeGIF должна применяться на протяжении всего жизненного цикла конкретной  
дискретной системы. Политики в отношении данных и метаданных

- XML должен быть основным стандартом для интеграции данных и управления ими для всех  
приложений в каждом министерстве, агентстве и органе власти Непала. Стандарты метаданных  
Непала должны быть в первую очередь основаны на международной дублинской базовой модели  
(ISO 15836) Разработка набора данных на национальном уровне и централизация метаданных  
страны должны быть выполнены в соответствии со стандартами совместимости метаданных

Политика безопасности

- достаточной зрелости в области доверенных вычислений и управления цифровыми правами (DRM) для обеспечения:

Конфиденциальности информации, находящейся в распоряжении правительства Непала

продолжать осуществлять контроль над данными правительства Непала и вычислительной средой

Защищать права на конфиденциальность, предоставляемые персоналу, использующему правительственные системы

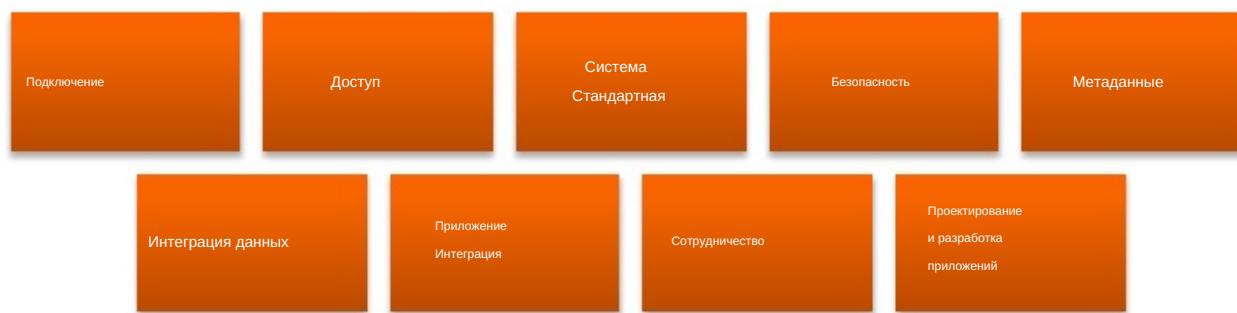
Обеспечивать конфиденциальность личной информации.

- Требования безопасности к информации, сервисам и инфраструктуре должны быть  
определенны и обработаны в соответствии с типом информации, условиями обслуживания и  
результатами анализа рисков Безопасность - это процесс,  
○ который должен присутствовать на всех этапах разработки приложения, рабочая группа по безопасности  
должна документировать системы, средства контроля безопасности и топологии среды  
, информировать каждый ИТ-отдел министерства / агентства об их ответственности за безопасность  
и правильное использование средств доступа, а также обновлять политику и процедуры

### 7.5.1 NeGIF - технические стандарты

NeGIF включает технические принципы, политику и стандарты, необходимые для достижения функциональной  
совместимости. Это минимальный набор, необходимый для поддержки ряда транзакций и услуг,  
предоставляемых правительством, и для интеграции информационных систем в рамках правительства.

Техническая политика охватывает следующие основные области, которые необходимы для взаимодействия:



Ниже приведен краткий обзор девяти технических областей и соответствующих компонентов.

Технические области	Компоненты
Взаимосвязь	<ul style="list-style-type: none"> <li>Интерконнекция -Telecom</li> <li>Сеть передачи данных доступа</li> <li>Сеть фиксированной связи следующего поколения</li> <li>Стандарты мобильной связи следующего поколения Межсоединение- предприятие</li> <li>Инфраструктура физического уровня Протоколы прикладного уровня Протоколы транспортного уровня Протоколы уровня Интернета Протоколы канального уровня</li> <li>Интегрированное соединение (телецентрическое предприятие)</li> <li>Стандарты интернет-провайдеров</li> <li>Стандарты Системы финансовой взаимосвязанности</li> </ul>
Интеграция данных	<ul style="list-style-type: none"> <li>Символы и кодировки для обмена информацией</li> <li>Описание данных</li> <li>Обмен данными и преобразование данных</li> <li>Форматы обмена данными</li> <li>Обмен информацией на основе онтологий</li> <li>Язык моделирования данных</li> <li>Метаязык интеграции данных Минимальный совместимый набор символов</li> <li>Оцифровка</li> <li>Определение данных для смарт-карт</li> </ul>
Безопасность	<ul style="list-style-type: none"> <li>Управление доступом</li> <li>Защита от нежелательной почты</li> <li>Антивирус / Шпионское ПО</li> <li>Брандмаэр рабочего стола</li> <li>Цифровая подпись</li> <li>Безопасность электронной почты</li> <li>Алгоритм шифрования</li> <li>Корпоративный брандмаэр</li> <li>Идентификация, аутентификация, авторизация и конфиденциальность</li> <li>Управление идентификацией</li> <li>Обнаружение и предотвращение вторжений</li> <li>Безопасность IP-инкапсуляции</li> <li>IP-безопасность</li> <li>Уровень безопасности 2</li> <li>Прокси-сервер</li> </ul>

Технические области

		Удаленная безопасность Инфраструктуры открытых ключей, Защищенный транспорт, VPN стандарты безопасности XML, Физическая безопасность,
		Маркер доступа, Анимация, Сжатие, Киоск, Мобильные устройства Скриптовая смарт-карта
		Доступ к каталогу Веб-доступ стандартный веб-браузер Рабочие станции Система электронной почты
		Управление корпоративным контентом IP-телефония Видеоконференции
		Разработка приложений для портативных устройств Структура разработки приложений Бизнес-правила, логика и объекты Проектирование и разработка моделей коммерческих готовых приложений (COTS) для географических информационных систем
Разработка приложений	Дизайн	&
		Язык программирования для разработки приложений, инструменты отчетности, Управление конфигурациями программного обеспечения (SCM), Сервис-ориентированная архитектура, Приложения для смарт-карт, Промежуточное программное обеспечение, ориентированное на сообщения, Посредники запросов объектов
		Удаленные вызовы процедур Серверы приложений Резервное копирование и восстановление Бизнес-аналитика Технология подключения к БД и доступа к ней СУБД Настольные операционные системы Службы каталогов Аппаратные платформы Управление ИТ-операциями Мобильные операционные системы Серверы портала Операционные системы серверов
		Устройства хранения данных Веб-сервер

Технические области

Спецификация  
сферы деятельности

для

конкретных целей

финансы  
Документооборот и  
веб-сервисы электронного  
здравоохранения ,  
электронного обучения,  
юридических кадровых  
электронных новостей

### 7.5.2 NeGIF - Стандарты данных

Рамочная программа взаимодействия электронного правительства (e-GIF) предусматривает принятие XML и разработку

XML-схем в качестве краеугольного камня государственной стратегии взаимодействия и интеграции. Ключевым элементом в разработке XML-схем является согласованный набор государственных стандартов данных (GDS). Стандарты данных

содержат подробное описание структуры объекта данных и его элементов данных.

Принятие стандартов данных для использования в государственных органах позволит упростить и повысить эффективность обмена данными и обработки данных. Это также устранит двусмысленности и несоответствия в использовании данных в правительстве, министерства, департаменты и правительства, агентства. Эти стандарты применяются ко всем системам, которые утверждены в NeGIF и предназначены для использования во всех других интерфейсах государственного сектора.

#### Каталог стандартов данных

Каталог стандартов данных излагает обоснование, подход и правила для установления и согласования набора государственных стандартов данных (GDS), которые будут использоваться правительством. Схемы данных и другие электронные средства обмена данными с участием государственного сектора, разработанные для поддержки e-GIF. Эти стандарты определены на логическом (бизнес-) уровне, а не на уровне физического хранилища базы данных. Однако рекомендуется использовать их для определения хранилища данных на бизнес-уровне.

Следующая структура / шаблон является рекомендательной для определения стандартов данных:

Название

Описание

Тип

Является Частью

Имеет Части

Формат и размер

данных, Версия

UML-диаграммы,

Идентификатор

XML-схемы, Проверки

Значений

Владелец

На основании

Статус

Проверка

Комментарии

Согласованная дата

Пример стандарта данных для объекта данных Сертификата гражданства приведен ниже в соответствии с указанным стандартным шаблоном data . Документ Каталога стандартов данных GEA в Непале предоставит полный список стандартов данных для идентифицированных общих и специфичных для сегмента объектов данных.

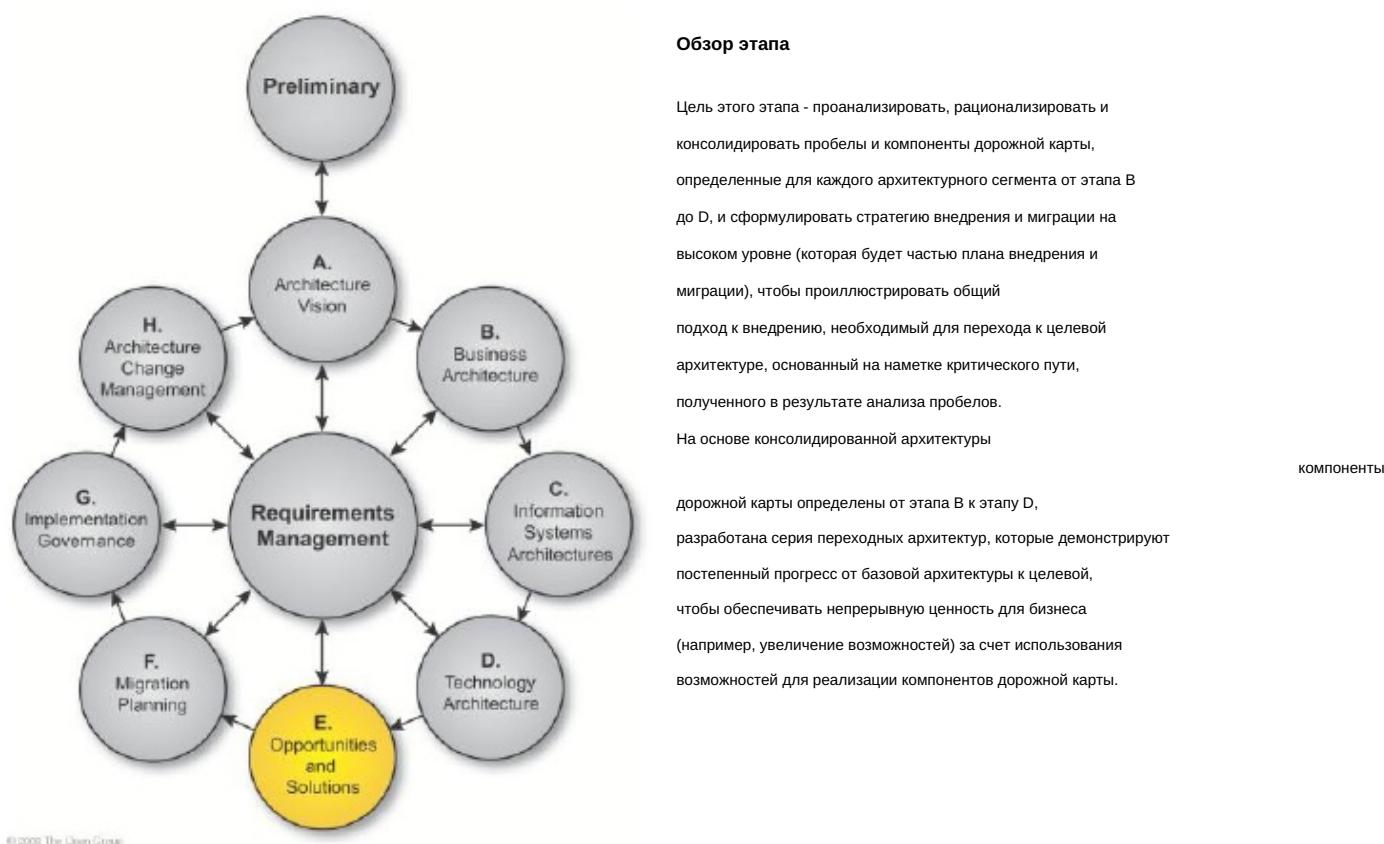
Метаданные	Значение
Имя	<b>Свидетельство о гражданстве</b>
Описание	Это специализированная форма элемента данных идентификатора участника, который содержит сведения о свидетельстве о гражданстве гражданина Непала.
Тип	Универсальный элемент данных
Является частью	Идентификатор участника (супертип)
Имеет часть	Идентификатор свидетельства о гражданстве (расширен от идентификатора участника) Тип гражданства (по рождению, усыновлению, наследственности и т.д.) Район выдачи свидетельства о гражданстве Адрес места рождения
Формат и размер данных	Обратитесь к формату и размеру отдельных дочерних элементов в Каталоге стандартов данных
Версия	1.0
Диаграмма UML	<pre> classDiagram     class PartyIdentifier {         -Party Identifier Type (Citizenship, Passport, PAN)         -Party Identifier Number         -Identifier Issuing Office : Office         -Identifier Issuing Date : Nepali Date         -Party Identifier Status         -Party     }     class CitizenshipCertificate {         -Citizenship Certificate Identifier : Party Identifier         -Citizenship Type (by birth, adoption, hereditary etc)         -Issuing District         -Birthplace Address : Address     }     PartyIdentifier &lt; -- CitizenshipCertificate   </pre>
Идентификатор схемы XML	Обратитесь к XML-схеме (xsd) <b>PartyIdentifierDescriptiveType</b> Обратитесь к определению XML <b>Сертификат гражданства</b> Структура
Проверки	Обратитесь к проверке отдельных дочерних элементов в Каталоге стандартов данных
Значения	Обратитесь к значениям отдельных дочерних элементов в Каталоге стандартов данных
Владелец	Министерство внутренних дел, Непал
На основе	
Подтверждение	<p><b>Если</b></p> <p>Свидетельство о рождении / свидетельство об образовании Свидетельства о гражданстве родителей</p> <p><b>потомок</b></p> <p>Документы, подтверждающие право собственности на недвижимость в Округе на имя семьи Или миграционное свидетельство, выданное соответствующим офисом CDO</p> <p><b>Если замужем за непальцем</b></p> <p>Свидетельство о гражданстве мужа Свидетельство о браке NOC из страны происхождения Документы, подтверждающие право собственности на недвижимость в Округе на фамилию Мужа ИЛИ Миграционное свидетельство, выданное соответствующим офисом CDO семье Мужа</p>

Метаданные	Ценность
	Рекомендательное письмо от председателя VDC / мэра / секретаря муниципалитета
Комментарии	
Статус	Подготовлено
Согласована дата	

Подробное описание рекомендуемых стандартов, спецификаций и протоколов NeGIF было рассмотрено в "Основном отчете NeGIF".

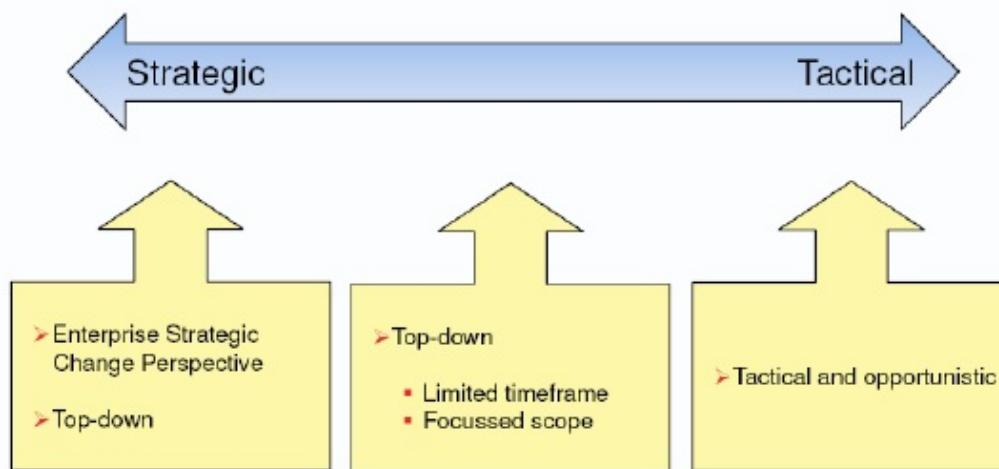
## ***8. Электронная фаза ADM TOGAF - Возможности и решения***

## 8. Фаза Е: возможности и решения



© 2008 The Open Group.

### 8.1 Возможности и решения для целевых архитектур



Первый этап, непосредственно связанный с тем, как будет реализована целевая архитектура

Корпоративный бизнес и техническая перспектива  
Рационализация ИТ-деятельности  
Объединение в пакеты работ по проекту

Консолидация, интеграция и анализ обширных исходных данных, включая

Существующие строительные блоки  
Тематические исследования  
Консолидированные результаты анализа пробелов

Упрощение за счет безжалостного сокращения

Количество создаваемых  
стандартных блоков Накладные расходы на  
управление портфелем и проектами

Создание высокоуровневой стратегии внедрения и миграции

Организация пакетов работ на  
критическом пути Распознавание зависимостей  
Со существование и интероперабельность  
Распознавание рисков и управление ими

Проведение анализа воздействия

Особенно на существующие ИТ-системы

### **Рационализированная и консолидированная Дорожная карта**

#### **Этапов В - D 8.2** Результаты анализа пробелов и компоненты дорожной карты для каждой из фаз

архитектуры, бизнеса, информационных систем и технологических архитектур (созданных на этапах В-Д) были проанализированы, их последствия оценены с точки зрения потенциальных решений / возможностей и взаимозависимостей, рационализированы и объединены в один длинный список, который становится основой для структуры разбивки работ и последующего определения архитектуры перехода.

Этап А	Этап В	Этап С
<b>Бизнес-архитектура</b>		
Униформа Подключение: 24x7 на всех уровнях правительства во всех министерствах / департаментах	Национальное хранилище данных: для безопасного и совместного хранения всего правительства. Данные из различных министерств / департаментов	электронные платежи Шлюз: для электронный перевод платы за услуги в правительство. Счета и для получения денежных средств от правительства

<p>Упрощение от Применения Формы: с ограниченным вводом данных и автоматическим извлечением данных из соответствующих баз данных</p>	<p>Автоматическая генерация идентификатора транзакции: для каждой онлайн-транзакции для применения отслеживания и использования в будущем</p>	<p>Цифровая копия сертификатов: для мгновенной проверки различных документов / инструментов (например, паспорта, водительских прав, земельного свидетельства и т.д.)</p>
<p>Механизм подачи услуг запросы: через Tele- центров, национальных портала и мобильных устройств</p>	<p>Общая инфраструктура обслуживания с использованием Телецентры: Поощрение различных министерств / ведомств тому, чтобы предоставлять свои Услуги G2C, B2C и B2B через Телецентры</p> <p>a. Разработка Модели подходящего для Бизнеса (например, ГЧП) для познакомиться капитальных и эксплуатационных затрат телекоммуникаций и для создания занятость возможностей</p> <p>b. Обеспечение оптимального охватывает (например, районы с высокой плотностью населения, которые необходимо иметь больше телекоммуникаций и т.д.) с. Стандартизация инфраструктуры и спецификаций подключения для телекоммуникаций после исходных данных получения подходящих данных из министерства / ведомства, услуги которых будут предлагаться через</p> <p>d. Телецентры, Реализующие Информационные материалы стратегию чтобы все были осведомлены о преимуществах, предлагаемых через Телецентры</p>	
<p>Интеллектуальная проверка данных заявителей: посредством электронного взаимодействия между различными министерствами / ведомствами для перекрестной проверки и обмена данными граждан</p>		
<p>Общегосударственная стратегия обучения: для государственного персонала различных уровней для обеспечения эффективного использования компьютеризированных систем</p>		
<b>Этап А</b>	<b>Этап В</b>	<b>Этап С</b>
<p><b>Архитектура данных</b></p>		
<p>Создание в данных архитектурные принципы, которые будут служить в качестве ключевых архитектурных исходных данных или движущих сил для правительственные организаций при проектировании будущей государственной архитектуры данных.</p> <p>Определение основных общих объектов данных предприятия и модели данных, которая представляет основные общие объекты данных, которые должны быть</p>	<p>Определение сущностей и модели данных для конкретных сегментов, необходимых для совместного использования данных и обмена ими в рамках системы интероперабельности для 16 включенных в краткий список подразделений по охвату.</p>	<p>Определение централизованного основного решения для центра управления данными, которое пытается централизовать и стандартизировать национальный основной набор данных путем точной консолидации, очистки, удаления дублирования и согласования основных данных, размещенных в разрозненных хранилищах данных. Это поможет поддерживать единую, надежную, точную, полную и последовательную</p>

используется в различных государственных подразделениях / департаментах правительства Непала для обмена данными & обмен в рамках структуры функциональной совместимости, устанавливающей государственные стандарты данных и метаданных NeGIF для основных общих объектов данных,		просмотр записей о гражданах и бизнесе в государственных подразделениях, которые могут быть единой точкой отсчета для других ведомств, что позволяет быстро и легко идентифицировать граждан в любой точке соприкосновения.
Завершает разработку целевой модели данных для сегмента IRD, включая любые дополнительные объекты данных, которые потребуются сверх объектов базовых данных для поддержки реинжиниринга процесса, как это было предложено командой PwC, Определение схемы государственных данных в формате XML для обмена		Поддержка и руководство командой по управлению данными в определении новых объектов данных, специфичных для сегмента, обновлении общих объектов данных и т. д. данные схема и стандарты данных, когда новые отделы будут готовы к интеграции с инфраструктурой GEA в Непале для предоставления новых электронных сервисов
данными и в рамках функциональной совместимости. Обмен платформа, которая будет основана на <b>Обычный выше спецификация.</b> Все департаменты, которые будут предоставлять свои государственные услуги как eServices, должны будут придерживаться рекомендуемой спецификации обмена общими данными определено в правительстве. XML- схема данных и пакет exchange (или определение контрактного обслуживания) для обеспечения бесперебойного информационного потока в eGIF, Формализующего модель и структуру управления данными		Определении схемы государственных данных в формате XML для <b>спецификации данных для конкретного сегмента</b> для обмена данными в рамках платформы взаимодействия. Конкретные департаменты, которые будут предоставлять свои услуги govt. как eServices, должны будут придерживаться рекомендуемой спецификации обмена данными для конкретного сегмента, как определено в Govt. XML-схема данных и пакет exchange (или определение контракта на веб-сервис) для обеспечения бесперебойного потока информации через eGIF
<b>Фаза А</b>	<b>Фаза В</b>	<b>Фаза С</b>
<b>Архитектура приложения</b>		
The Сеть инфраструктура соединения GIIDC / NITC со многими другими подразделениями не существует. Поскольку уровень интеграции будет находиться в NITC, это должно быть связано с приложениями отдела, к которым будет подключаться уровень интеграции.	За исключением нескольких приложений (таких как системы управления регистрацией лицензий , PIS, ePAN и т.д.), они имеют четко абстрагированный бизнес- логический уровень. Требование бизнес-логики / сервиса важно для веб-сервиса	Приложение в настоящее время могут быть внедрены возможности для критически важных приложений для мониторинга работоспособности систем.

Например: Избирательная комиссия в настоящее время не подключена к сети с NITC.	включите бизнес-логику.	
Некоторые из в приложений, особенно приложения типа 1 нуждаются в перепроектировании для переноса на базовые онлайн-приложения. Приложения типа 2 для тех, которые являются клиент-серверными приложениями, также должны быть подключены к Интернету.	Обычный Применение Необходимо развернуть аутентификацию и авторизацию .  Большинство отдел приложений бы необходимо повторно-проектирование для интеграции с уровнем интеграции GEA.	
<b>Фаза А</b>	<b>Фаза В</b>	<b>Фаза С</b>
<b>Архитектура интеграции</b>		
NGSDG обеспечит использование сервис-ориентированной архитектуры (SOA) и будет действовать как корпоративная сервисная шина для всех взаимодействий между потребителями услуг (гражданами и предприятиями) и различными поставщиками услуг (правительственными ведомствами) и даже между правительственными ведомствами.	Предоставляет необходимые соединители для взаимодействия с приложениями, разработанными на уровне отдела . Способен обрабатывать большое количество транзакций по всей сети, предоставлять данные и форматировать преобразование, если таковое имеется, наряду с маршрутизацией и фильтрацией данных.	Общие сервисы - В будущем в сервиснойшине SDG Enterprise Service Bus появится возможность добавлять дополнительные функциональные возможности для поддержки общих сервисов, таких как аутентификация, платежный интерфейс шлюза, службы коротких сообщений, службы мгновенного обмена сообщениями и т.д.
Предоставление услуг для приложений отдела с помощью NGSDG новые и устаревшие приложения отдела могут предлагать свои услуги различным другим потребителям, подключенным к корпоративной сервисной шине.	Облегчите синхронизацию в режиме реального времени и почти в режиме реального времени и координацию межведомственной работы, отслеживая все транзакции правительства Непала.	
Обеспечьте общий набор интеграционных спецификаций и единую точку доступа.		
Безопасность и аудит - Результаты в улучшении отслеживания (аудит) и безопасность каждого вызова службы и обеспечивает государственный контроль посредством полных журналов аудита и временной отметки транзакций		
<b>Фаза А</b>	<b>Фаза В</b>	<b>Фаза С</b>
<b>Архитектура Безопасности</b>		
Регистрация: единую централизованную регистрацию для всех приложений	Проверка Подлинности Приложения	Централизованное: следует использовать
		Администрирования: утилита администрирования для всех
Централизованное		

	централизованный механизм. Для аутентификации не должно использоваться локальное хранилище	аутентификация пользователя	приложение в организации
Федеративная аутентификация:  Система должна иметь возможность использовать централизованную схему аутентификации , а также аутентификацию на основе приложений	Целостность: Все приложения должны иметь безопасность сеансового уровня	Извещения о событиях с помощью определите и отправьте это	Уведомления: повышение безопасности серьезность
Единая точка доступа: единая точка входа для всего приложения	основанная Авторизация: на политике Авторизация должна быть управляемая из центрального пользовательского хранилища.		
Идентификация: Должен быть уникальный идентификатор для всех пользователей и приложения	Конечное Конечная целостность: приложение должно использовать безопасность на транспортном уровне при взаимодействии с другим приложением.		
Сканирование приложений: Все приложения должны быть просканированы на наличие какой-либо уязвимости.	Аудит: Все приложения должны иметь функцию аудита для отслеживания того, кто выполнял определенное действие и когда.		
Повышение надежности конфигурации: Все приложения и аппаратные средства должны быть настроены таким образом, чтобы свойство по умолчанию не создавало никаких рисков для окружающей среды.	Отказ от ответственности: Приложение должно быть способно представить доказательства происхождения данных и получателя данных Политика безопасности:		
	Необходимо разработать политику безопасности информации, данных и приложения		
<b>Этап А</b>	Фаза В	Фаза С	

**Архитектура инфраструктуры**

Консолидация центров обработки данных	Внедрение общей сети	Конфигурация База данных	Руководство
Безопасность  а. Общие службы безопасности б. Инфраструктура в. Сетевая безопасность г. Защищенный сегмент	Государственная глобальная сеть		Управление инфраструктурой
	Государственный центр обработки данных  Эксплуатация центра обработки данных и системное управление - ITIL  Соображения безопасности б. для центра обработки данных с. Безопасность центра данные		

	Структура Автоматизация центров обработки данных d.	
--	---	--

## Стратегия внедрения и миграции на высоком уровне 8.3

На основе приведенных выше консолидированных и рационализированных дорожных карт отдельных архитектур разрабатывается

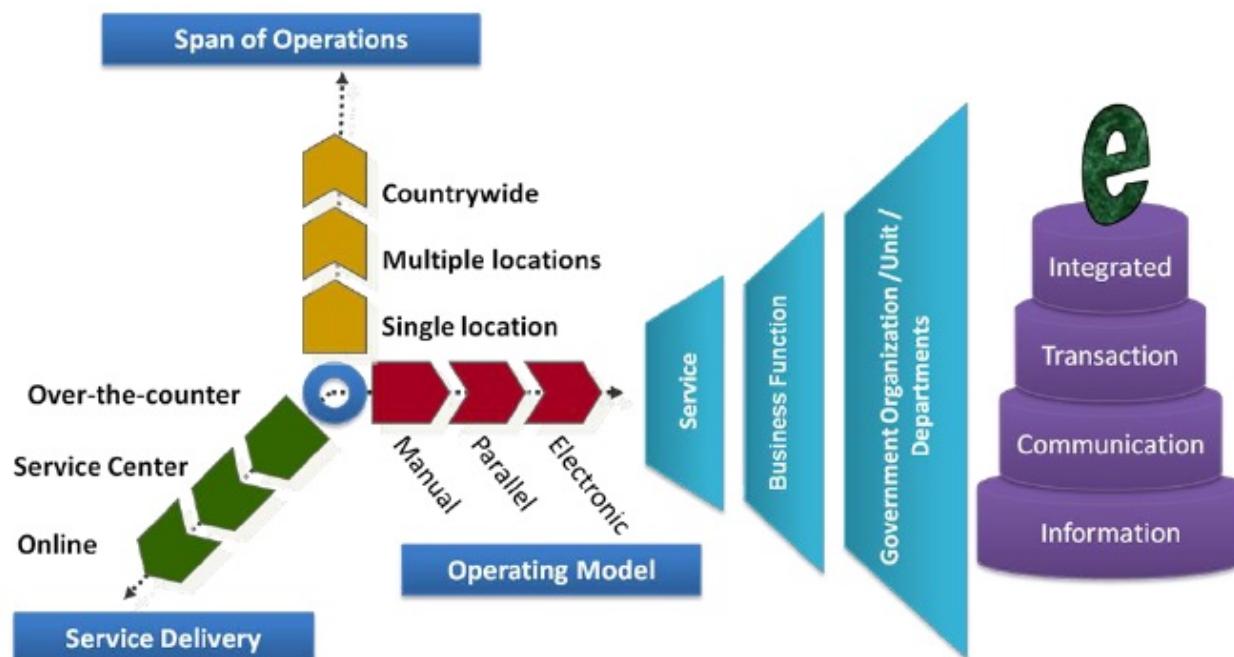
общая стратегия и подход к реализации / решениям, которые будут определять реализацию целевой архитектуры и структуру  
переходных архитектур..

Согласно предлагаемой стратегии внедрения, предоставление государственных услуг гражданам в виде электронных  
услуг, как правило, будет осуществляться поэтапно в зависимости от существующих прикладных систем и сетевой  
 зрелости инфраструктуры каждого департамента в использовании предлагаемой инфраструктуры предоставления услуг для  
предоставления своих услуг. Цель состоит в том, чтобы предоставить гражданам немедленную возможность отправлять формы запросов  
на получение онлайн-услуг , определенные департаментами на национальном портале. На основе режима  
работы подача, обработка и отслеживание статуса выполнения услуг будет осуществляться либо -

В Национальном портале, Если ведомства не удается подключиться к службе шлюза доставки

В ведомственных системах, если ведомства могут подключаться к шлюзу предоставления услуг

Переход от ручного к электронному режиму работы, будущая модель предоставления  
государственных услуг проиллюстрирована ниже -



### Операционная модель предоставления услуг

Операционная модель предоставления электронных услуг с национального портала через

электронные формы, как правило, переходит от ручного к электронному -

- Руководство

- На национальном портале будут размещены электронные формы государственных услуг.  
Граждане могут войти на национальный портал, заполнить и отправить форму.

- Национальный портал будет хранить и фиксировать запрос на обслуживание в инфраструктуре портала, которая будет служить центральным приложением для сбора запроса на обслуживание.
- В подразделениях нет какой-либо прикладной системы и сетевой инфраструктуры для подключения к шлюзу доставки eService. Назначенное лицо загрузит запрос на обслуживание с национального портала и начнет обрабатывать его вручную в соответствии с текущим процессом департамента.
- Параллельно
  - На национальном портале будут размещены электронные формы государственных услуг. Граждане могут войти на национальный портал, заполнить и отправить форму.
  - Национальный портал будет хранить и фиксировать запрос на обслуживание в инфраструктуре портала, которая будет служить центральным приложением для сбора запроса на обслуживание.
  - Ведомственная система подачи заявок существует, но не интегрирована со шлюзом доставки eService. Назначенное лицо загрузит запрос на обслуживание с национального портала и начнет его обработку через ведомственную систему.
- Электронный
  - На национальном портале будут размещены электронные формы предоставления государственных услуг. Граждане могут войти на национальный портал, заполнить и отправить форму.
  - Национальный портал опубликует запрос на обслуживание непосредственно в шлюзе доставки eService.
  - Ведомственная система интегрирована со шлюзом доставки eService и способна принимать запрос на обслуживание и обрабатывать его.

#### Каналы предоставления услуг

Каналы предоставления услуг обычно переходят от -

- "Вручную - без рецепта"
  - Это типичный ручной процесс, при котором форма запроса на обслуживание будет собираться, заполняться и отправляться гражданами вручную без рецепта
- Полуавтоматический - Сервисные Центры
  - Это полуавтоматический подход, при котором граждане, находящиеся в удаленном месте, могут воспользоваться услугой запроса услуги, предоставляемой местными центрами обслуживания (аналогично телекоммуникациям), которые будут способствовать онлайн- отправке форм от имени гражданина. Все подтверждающие документы будут переданы сотрудникам сервисного центра для проверки.
- Электронный - Онлайн через Национальный портал
  - Граждане могут напрямую воспользоваться онлайн-сервисом на национальном портале, заполнить и отправить форму, загрузив подтверждающие документы.

#### 8.4 Архитектура перехода к идентичности

На основе рационализированных и консолидированных компонентов дорожной карты архитектуры, определенных от этапа B до D в разделе 8.2, разработан ряд переходных архитектур, которые демонстрируют постепенный прогресс от базовой архитектуры к целевой, обеспечивающей непрерывную ценность для бизнеса (например, увеличение производственных возможностей) за счет использования возможностей для реализации компонентов дорожной карты.

Для полного преобразования предлагаемого GEA в Непале с базового на целевой будет применяться поэтапный подход, начиная с перехода от базовой архитектуры к целевой для правительства Непала. Преимущество использования подхода с архитектурой поэтапного перехода заключается в том, что правительство / организации считают, что изменение архитектуры оказывает слишком большое влияние на организацию, чтобы его можно было осуществить за один этап.

Ниже приведены ориентировочные идентифицированные фазы / переходные состояния. Временные рамки переходного состояния / фаз, упомянутых здесь, будут зависеть от Руководящего комитета GEA и готовности отдельных проектов / программ в области ИКТ департаментов. Этот раздел поэтапного подхода отражает ориентированную последовательность проектов, которые необходимо реализовать, чтобы избежать конфликтов зависимости проектов и решений.

Переходное состояние 1 (фаза А)	Переходное состояние 2 (фаза В)	Переходное состояние 3 (фаза С)
<p>1. Установить Непал eService Промежуточное программное обеспечение шлюза доставки платформа, основанная на SOA, для всех взаимодействий между потребителями и поставщиками услуг</p> <p>2. Развертывание Mule ESB с безопасностью / аудитом</p>	<p>1. Mule для обеспечения необходимых соединителей для взаимодействия с приложениями отдела</p>	<p>1. Добавьте общие сервисы, такие как интерфейс платежного шлюза и т.д.</p> <p>2. Интеграция со шлюзом ePayment</p>
<p>3. Национальный портал, развернутый с статический контент</p>	<p>2. Национальный Портал Для постепенно размещайте eServices постепенно с централизованной регистрацией пользователей (LDAP для всех приложений с уникальным на основе) идентификатором для всех пользователей и приложений</p>	<p>3. Национальный Портал Для поэтапное размещение электронных сервисов</p>
<p>4. Настройка от централизованного пользователя регистрации (на основе LDAP) для пользователей национального портала</p> <p>5. Федеративная аутентификация принятый подход</p>	<p>4. Постепенно переходите к централизованная аутентификация Принудительное использование функций на основе политик 5. авторизация будет контролироваться из центрального хранилища пользователей</p> <p>6. Обеспечить безопасность на уровне отказа</p>	<p>4. Принудительное использование функций цифровой подписи и инфраструктуры</p> <p>5. PKI Оповещений и уведомительных функций</p>
<p>6. Установить общий для информации данных стандартными</p>	<p>8. Установить конкретные сегмент стандарт данных для обмена информацией 9. Определение и публикация сегмента</p>	<p>6. Установить Национальный Обмен данными репозиторий</p>
<p>7. Определите и опубликуйте государственную XML-схему данных.</p>	<p>7. конкретная Государственнные XML схема</p>	<p>7. ofSetup Основное данными решение для управления</p>
<p>8. Настройка инфраструктуры GIDC на размещение ESB и национального портала</p>	<p>10. GIDC для размещения другого проекта в области ИКТ приложения для департаментов</p>	
<p>9. Создание сетевого руководства и приложения 24 * 7 подключение к отдел</p>	<p>11. Настройка на территории Непала сети 12. Установите 24 * 7 сеть подключения с GIDC и другие приложения</p>	<p>8. Установить связь с телецентрами</p>

Переходное состояние 1 (фаза А)	Переходное состояние 2 (фаза В)	Переходное состояние 3 (фаза С)
<p>10. Пилотное внедрение с IRD с национальным порталом для размещения IRD eServices 11. Данные, относящиеся к конкретному сегменту будут определены стандарты для IRD</p> <p>12. Веб-сервисы для электронных сервисов IRD будет определен</p> <p>13. Включение службы ESB в IRD веб-сервисы 14. Национальный портал обеспечить интерфейс для граждан, бизнеса и департаментов для использования электронных услуг IRD</p>	<p>13. Отделы завершением / близки к завершению в области ИКТ (например, ЕС, Непальская полиция, NTA, FCGO и т.д.) Для подключения к шлюзу предоставления услуг</p> <p>14. Веб Услуги Для В ESB-сервисы для конкретных подразделений будут определены</p> <p>15. ESB-сервис, позволяющий услуги конкретные веб-департамента</p> <p>16. Национальный портал для предоставления услуг интерфейс для граждан и бизнеса для предоставления электронных услуг, специфичных для конкретного департамента</p> <p>17. Национальный портал, обеспечивающий интерфейс для других отделов без использования приложений, специфичных для конкретного отдела сервисы для конкретного отдела 18. Обслуживание Для ESB потребители (другие контакты) инфраструктура Для пользоваться электронными услугами, специфичными для конкретного подразделения</p>	
<p>15. Формализовать EA Управление Модель 16. Департаменты</p>		

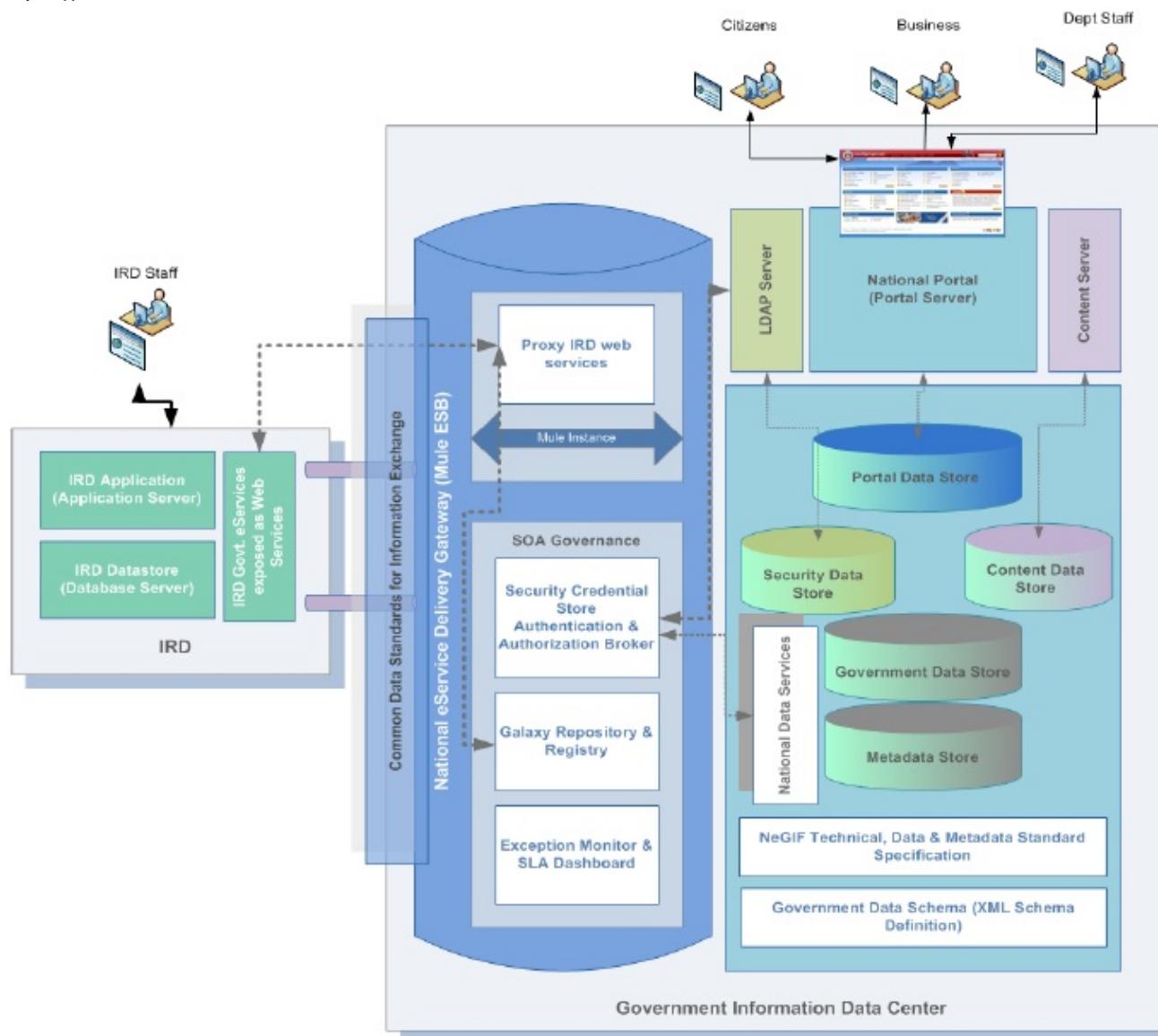
с проектами в области ИКТ на различных стадиях зрелости в соответствии с GEA и eGIF Непала

спецификация

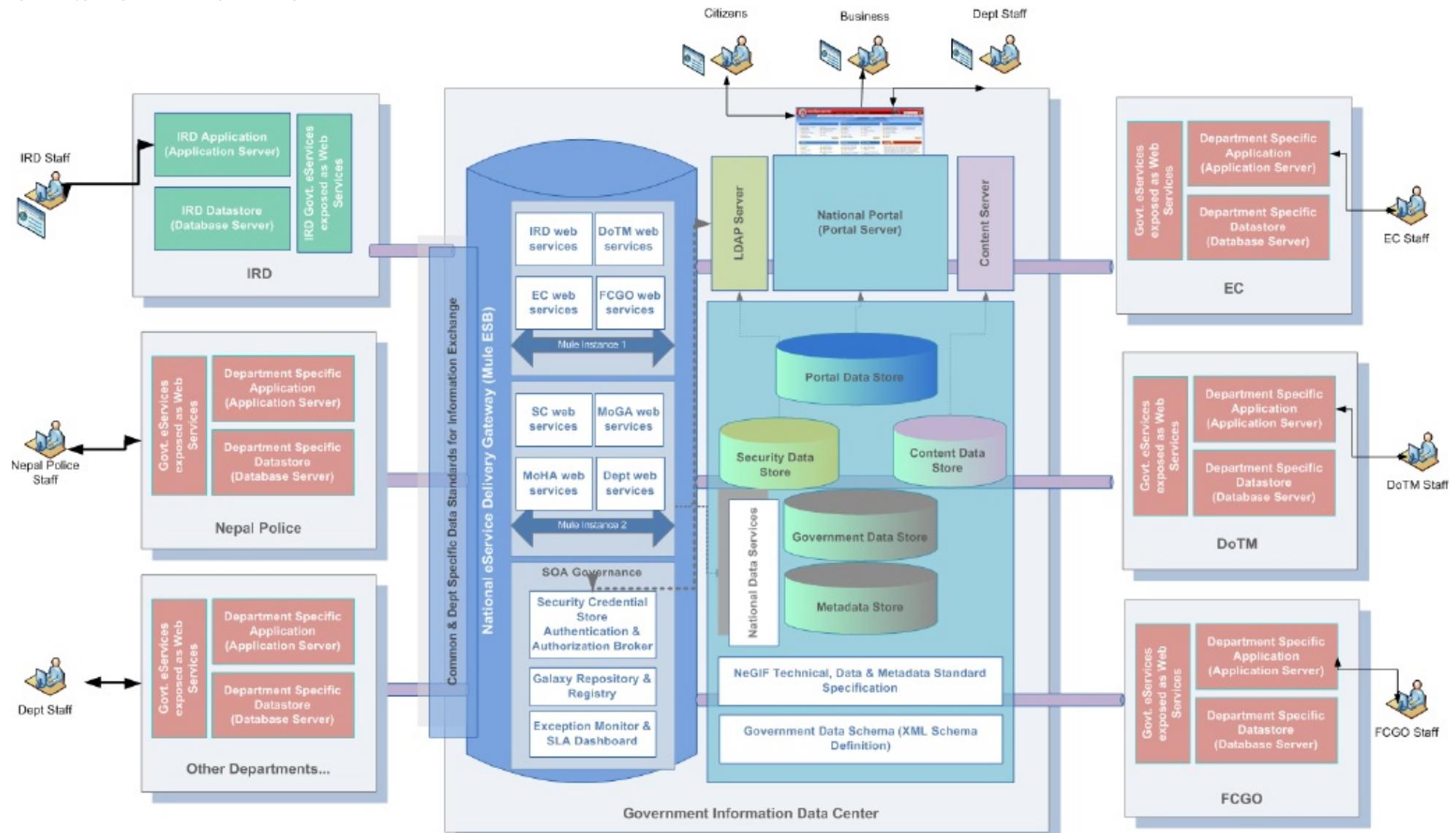
17. Проектирование / редизайн на основе спецификаций GEA

18. Руководящий комитет GEA по рассмотрению проекта и обеспечению соответствия спецификациям GEA

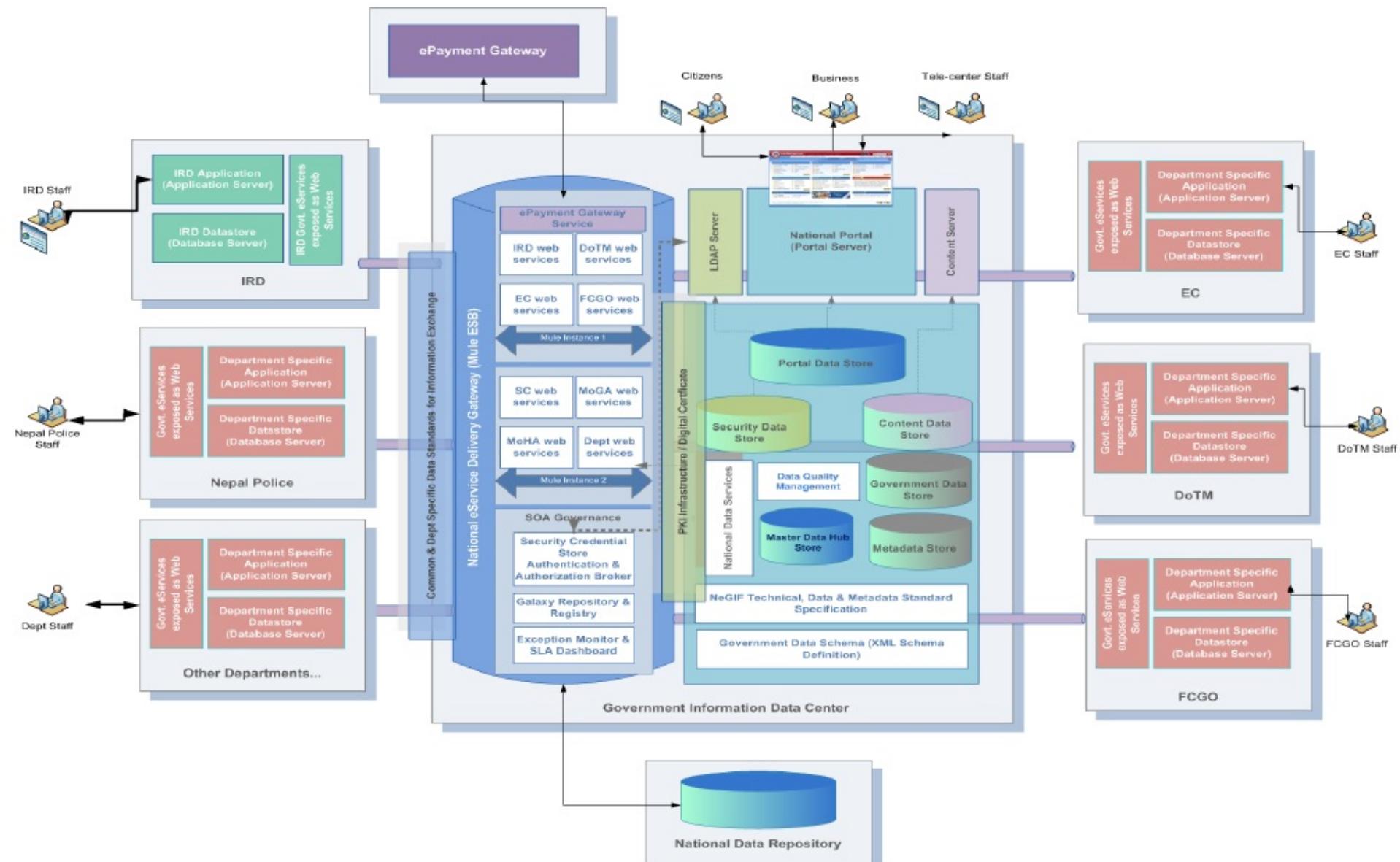
Архитектура переходного периода - переходное состояние 1



Архитектура переходного периода - переходное состояние 2



Архитектура переходного периода - Переходное состояние 3



## 8.5 Создание Портфолио и Уставов проектов

Основываясь на архитектурах перехода, разработанных для постепенного продвижения от базового уровня к целевому, подход на этом этапе заключается в завершении портфолио и основных уставов проектов, при этом их конечные результаты группируются по этапам и планируются к выпуску в рамках этапов перехода к архитектуре. Эти архитектуры обеспечивают корпоративный контекст, позволяющий проектам приступать к разработке методологии разработки системы этапы инициирования, планирования и оценки требований. Основным мероприятием на этом этапе является обзор и консолидация портфолио и потенциально основных уставов проектов и обеспечение четкого определения их архитектурных результатов. Эти архитектурные результаты зададут корпоративный контекст портфеля и определят "соответствие" и "ценность" результатов для управления. Список стратегических портфелей / проектов, которые будут сгруппированы в рамках каждого переходного этапа, будет зависеть от руководящего комитета GEA и готовности каждого департамента к конкретным программам / проектам в области ИКТ.

## **9. Фаза F TOGAF ADM - Планирование миграции**

## 9. Фаза F: планирование миграции



Определение **Дорожная карта внедрения и миграции** для Непала инициатива GEA потребует значительного вклада, участия, сотрудничества и координации между правительственными ведомствами и Руководящим советом GEA и зависит от зрелости и готовности конкретных программ / проектов GEA в области ИКТ со стороны департамента. Этот этап будет более применимым и завершенным на более позднем этапе, как только будут доработаны различные строительные блоки (проекты / программы в области ИКТ) архитектуры переходного периода. Однако краткий подход, обычно применяемый на этом этапе, был изложен ниже в качестве руководства для департаментов, инициирующих новые проекты / программы в области ИКТ.

### 9.1 Ценность для бизнеса каждого Проекта

Подход на этом этапе заключается в установлении и присвоении бизнес-ценностей всем проектам в области ИКТ и приращениям проекта . Цель состоит в том, чтобы сначала установить, что представляет собой ценность для бизнеса в организации, как ее можно измерить, а затем применить это к каждому из проектов и приращениям проекта.

### **Оценки потребностей в ресурсах и сроков реализации**

**проекта. 9.2** Подход на этом этапе заключается в определении требуемых ресурсов и сроков для каждого проекта и его приращения и предоставлении первоначальной сметы затрат на проекты. Затраты должны быть разбиты на капитальные (для создания потенциала) и операционные и эксплуатационные (для запуска и поддержания потенциала). Обратите внимание, что финансирование операций и технического обслуживания должно начаться сразу после поступления первого взноса в организацию по управлению операциями, поэтому с самого начала должно быть ясно, откуда поступают оба вида финансирования (и являются ли они доступными). Отличными примерами проблем являются стоимость обслуживания программного обеспечения и затраты, связанные с обновлением (включая некоторые пользовательские модификации программного обеспечения, которые были внесены).

### **9.3 Определение приоритетов миграционных проектов**

Целью этого этапа является определение приоритетов проектов путем определения коммерческой ценности артефактов, поставляемых проектами, в сравнении со стоимостью их доставки. Подход заключается в том, чтобы сначала как можно четче определить чистую выгода от всех решений, предлагаемых проектами, а затем убедиться в том, что риски были эффективно снижены и учтены. Впоследствии цель состоит в достижении необходимого консенсуса (часто на уровне предприятия) для составления списка приоритетных проектов, который послужит основой для распределения ресурсов. Критерии приоритизации будут включать ключевые бизнес-факторы, определенные на этапе E, а также те, которые относятся к повесткам дня отдельных заинтересованных сторон.

Некоторые из ключевых критериев расстановки приоритетов, которые можно было бы рассмотреть, включают в себя::

Будет иметь высокую видимость при внедрении.

Повысит эффективность (за счет увеличения времени выполнения заказа, за счет

упрощения потоков и т.д.) Процесса

участники Способность заинтересованных

сторон справляться с изменениями, будут ли заинтересованные стороны готовы принять их

и адаптироваться к

измененный процесс и услуги

снизит общие затраты получателей на пользование услугой

Повлияет на большое количество

заинтересованных сторон Консолидация услуг

Целью иметь минимум "промежуточных" решений (они часто становятся долгосрочными / стратегическими!). Было бы

Долгосрочное решение, которое может сохраняться в

течение приемлемого периода времени Будет иметь подходящие ИТ-системы для поддержки

реинжиниринга и управлению подходящих веб-сервисов

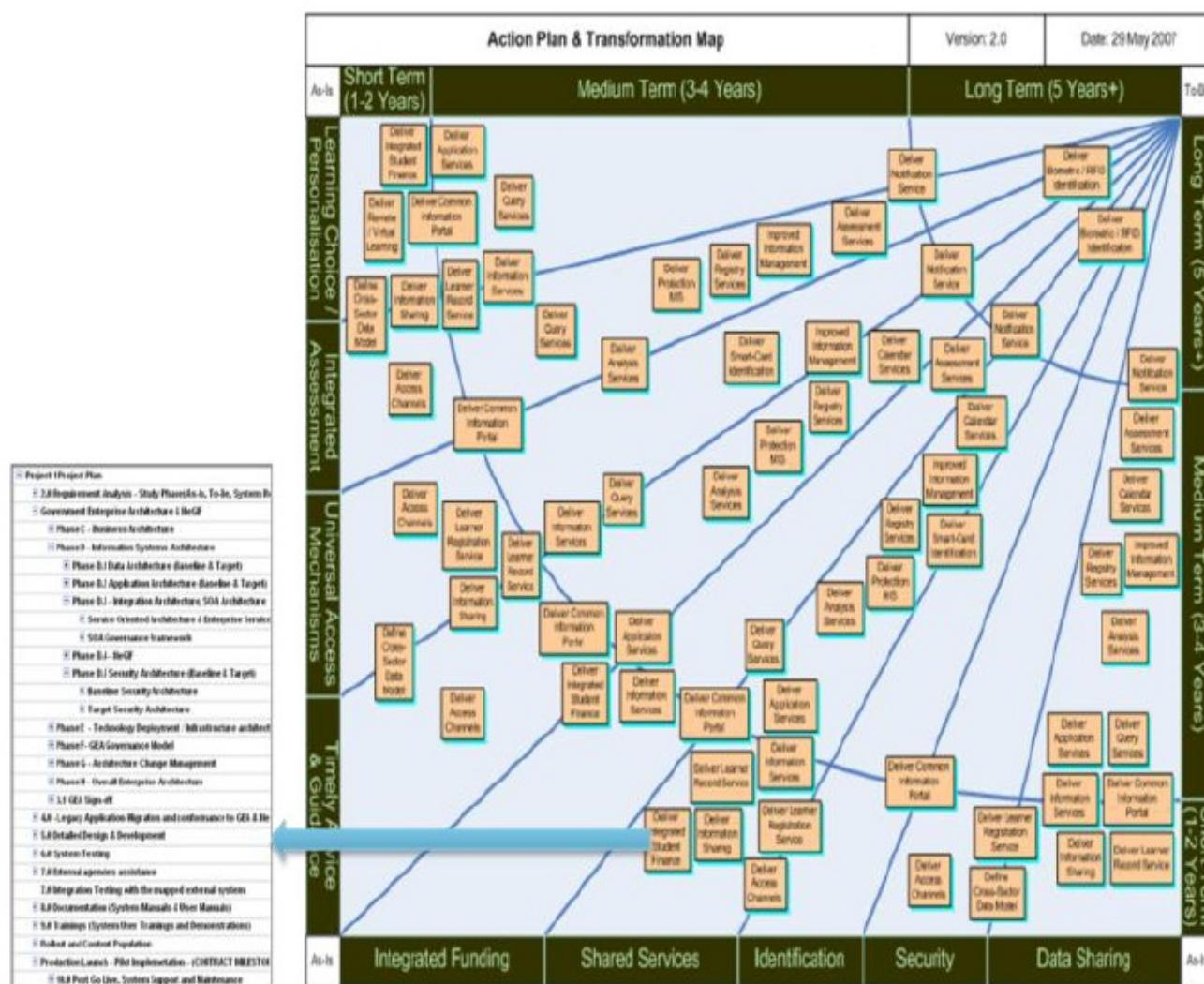
### **Дорожная карта внедрения высокого уровня и миграция 9.4**

#### **План**

Целью этого шага является создание последовательности и деталей плана внедрения и миграции. Основная особенность архитектурного планирования заключается в том, что будет много параллельных проектов / программных мероприятий в области ИКТ, и План внедрения и миграции будет связывать все эти артефакты воедино. На этапе E и на предыдущих этапах в рамках этапа F большая часть действий по планированию проекта / портфеля проектов будет завершена, и на этом этапе все детали объединяются в общий план. На этом этапе основной задачей является формальная интеграция всех проектов, этапов проекта и действий, а также зависимостей в план проекта, предпочтительно с использованием инструмента планирования проекта и управления, который использует стандартную методологию, такую как метод критического пути или тому подобное. Государства переходной архитектуры с их

определенная стоимость бизнеса будет выступать в качестве контрольных точек портфеля. Также необходимо убедиться, что все внешние зависимости захвачены и включены. Например, задержка с завершением и формализацией правовой базы NID и последующая реализация проекта NID могут привести к тому, что проект EC в области ИКТ в рамках архитектуры раннего переходного периода будет отдан приоритет государству, рассматривающему профиль избирателей EC в качестве надежного источника данных о гражданах. Кроме того, график проекта также должен быть включен в план. Проекты должны выполнять возложенные на них роли и обеспечивать тщательное планирование результатов. Их проектные планы должны быть частично включены (частично или полностью) в План внедрения и миграции. Корпоративному архитектору рекомендуется обеспечить соответствие плана общему плану внедрения и миграции с учетом проблем проекта, если таковые имеются, чтобы у него было больше шансов на успех. Результатом этого действия является окончательный план внедрения и миграции.

Типичный пример дорожной карты внедрения и плана миграции показан ниже -



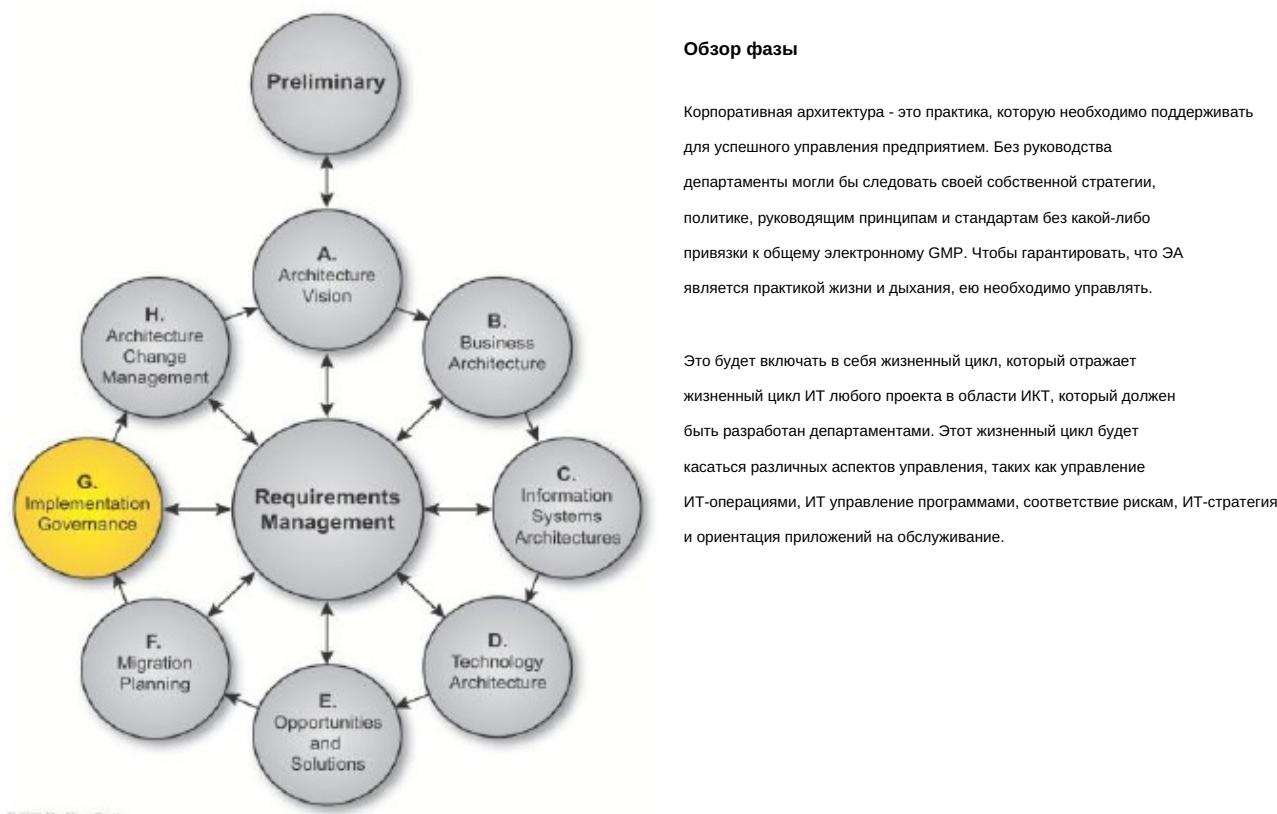
## 9.5 Цикл эволюции архитектуры

Корпоративные архитектуры необходимо поддерживать в актуальном состоянии, иначе они постепенно утратят актуальность и будут вытеснены портфолио и / или проектными архитектурами. Время, необходимое для перехода от стратегической архитектуры к архитектуре проекта , является значительным, и его необходимо понимать и учитывать в организации. Кроме того, извлеченные уроки имеют решающее значение в обучающейся организации и должны быть задокументированы и оценены как часть процесса эволюции предприятия. Цикл эволюции архитектуры будет как влиять, так и регулироваться управлением изменениями архитектуры предприятия (фаза H).

## **10. Фаза G TOGAF ADM -**

### **Управление архитектурой**

## Фаза G: архитектура 10. Управление



Следующий рисунок иллюстрирует различные аспекты общего управления ЭО в стране. Для каждого из аспектов также указана методология.

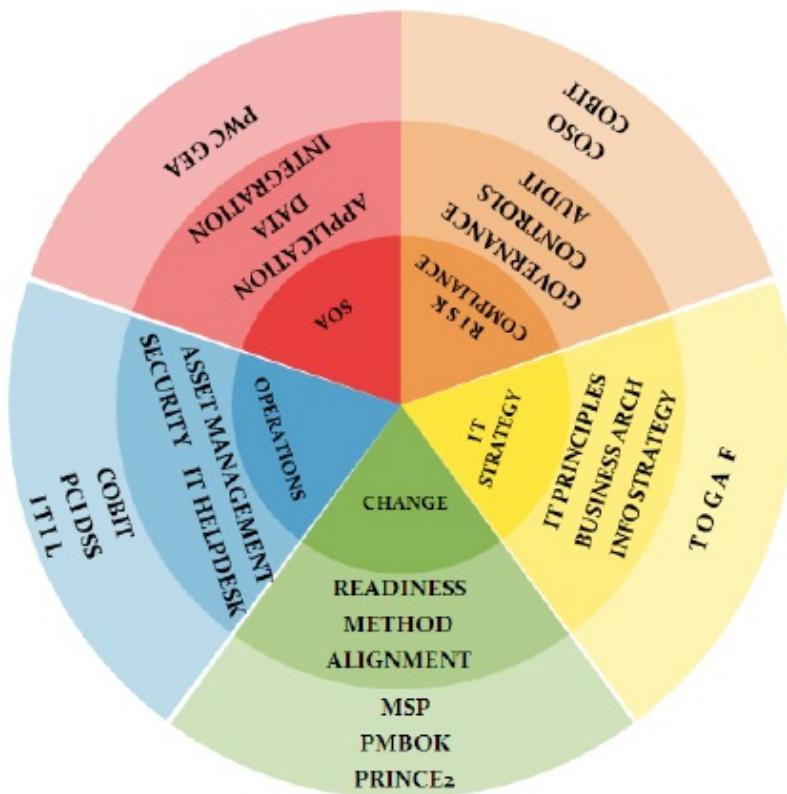


Рисунок GEA Непала - Аспекты управления

Жизненный цикл будет включать определенных участников / роли в разных подразделениях на разных этапах, чтобы гарантировать, что архитектура предприятия (EA) и Структура взаимодействия электронного управления (NeGIF) соблюдаются и приведены в соответствие с общими целями проектов в области ИКТ. Следующий рисунок иллюстрирует различные этапы в достижении общей зрелости ИТ и электронного управления и соответствующих механизмов управления.

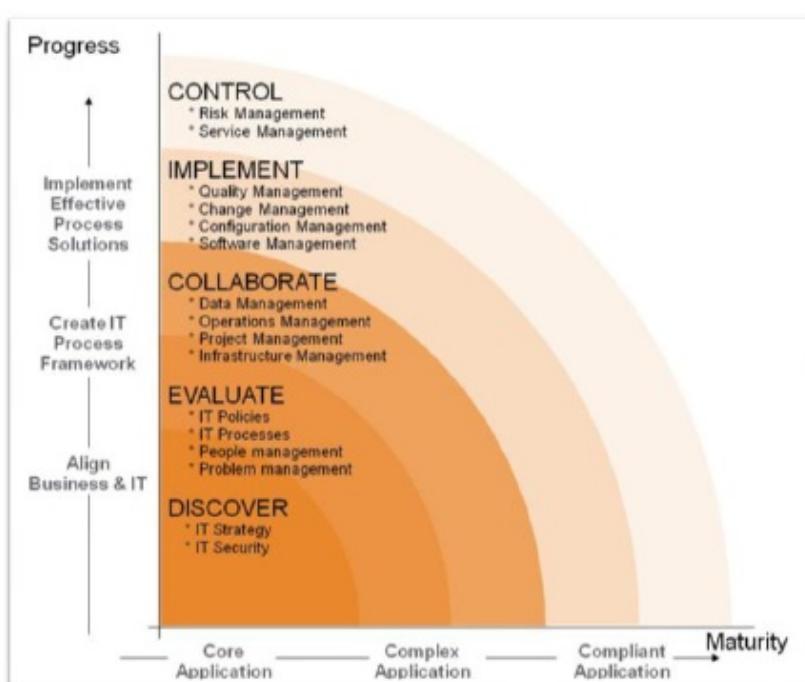


Рисунок: GEA в Непале - Этапы управления

## Цели

Целью этого этапа является формулирование рекомендаций по каждому проекту внедрения, а также регулирование и управление контрактом на архитектуру, охватывающим общее внедрение и развертывание системы. Затем система внедряется и развертывается на этом этапе. Ниже приведен список целей.

Сформулируйте общие рекомендации по архитектуре, которые будут использоваться в каждом проекте внедрения. Соблюдение модели устойчивого управления для реализации любого проекта в области ИКТ. Создайте архитектурный контракт для управления общим процессом внедрения. Выполнять соответствующие функции проверки со стороны руководства во время внедрения и развертывания новых систем. Обеспечивать соответствие определенным архитектурным стандартам в рамках проектов внедрения.

## Подход

На этом этапе собирается вся информация для успешного управления различными проектами внедрения

Рекомендуемый подход заключается в развертывании целевой архитектуры в виде серии постепенных переходов, каждый из которых сам по себе приносит пользу бизнесу:

- Разработать программу внедрения, которая позволит осуществить Переходный период ○ Архитектуры, согласованные для внедрения на этапе планирования миграции,
  - Предусматривают поэтапный график развертывания, который отражает бизнес-приоритеты, воплощенные в ○ Дорожная карта архитектуры.
  - Следуйте стандартам организации в области корпоративного управления, информационных технологий и архитектуры ○ Используйте устоявшийся в организации подход к управлению портфелем / программой, где он существует
  - Определите операционную структуру для обеспечения эффективного длительного срока службы развернутого решения На этом этапе устанавливается связь между архитектурой и организацией внедрения
    - Использование архитектурного контракта
- Управление внедрением тесно связано с общим управлением архитектурой
- Ключевым аспектом этапа является обеспечение соответствия определенной архитектуре (ам)
- Проекты внедрения
  - Другие текущие проекты внутри предприятия

Управление архитектурой предприятия - это совокупность нескольких функций управления архитектурой, таких как SOA управление, Управление данными, управление приложениями, управление технологиями / инфраструктурой и управление ИТ-безопасностью . У каждого из этих органов управления есть свой жизненный цикл, которым необходимо управлять с определенными ролями, обеспечивающими соблюдение стандартов на отдельных этапах.

## 10.1 Потребность в управлении GEA

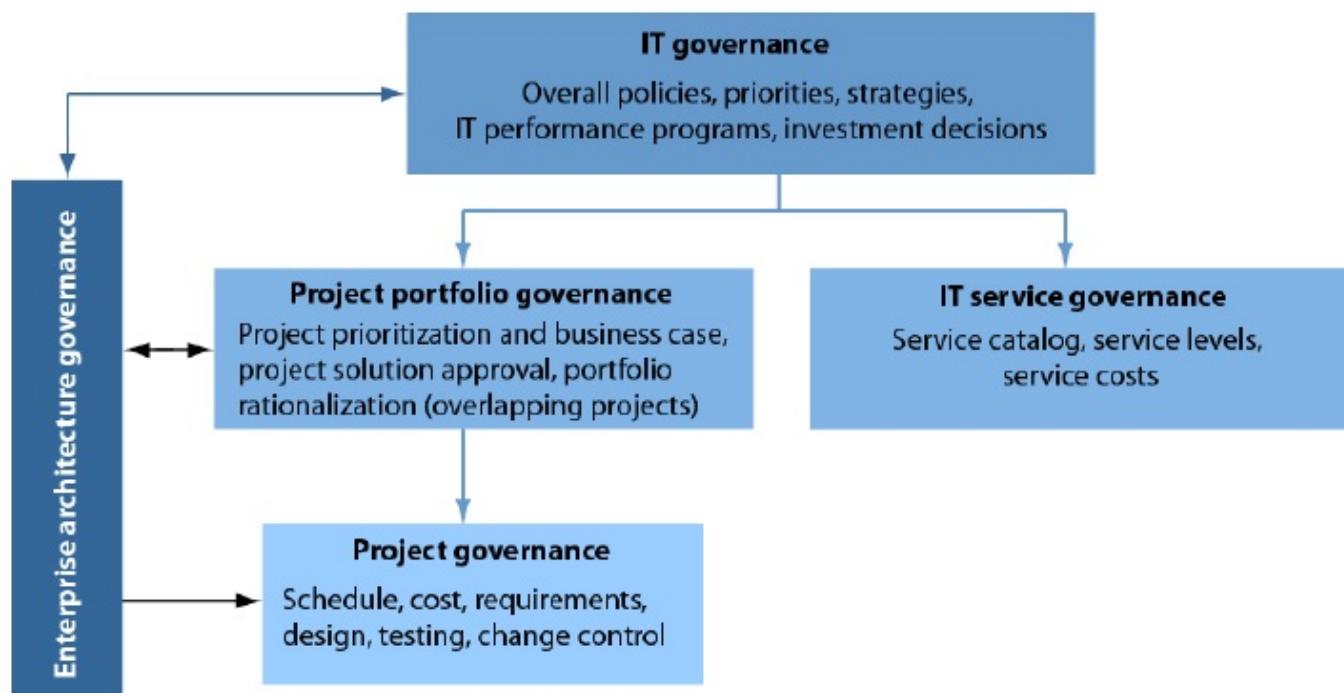
### управлении GEA

Повышение эффективности архитектуры предприятия сопряжено с существенной проблемой попыток повлиять на поведение персонала, находящегося вне прямого контроля, что влечет за собой серьезные политические трудности, которые могут подорвать все усилия.

Периодический обзор является критическим для определение что есть работает и что должен улучшение. Архитектурные группы, которые пытаются двигаться вперед без регулярной обратной связи об их ценности для своей организации, рисуют растратить свои ресурсы вместо того, чтобы сосредоточиться на областях с высокой отдачей. После определения архитектур необходимо спланировать, как архитектура перехода, реализующая архитектуру, будет регулироваться в процессе внедрения.

## 10.2 Введение и подход к управлению EA

Управление архитектурой предприятия является частью управления ИТ на нескольких уровнях



Управление ИТ определяет, как архитектура предприятия вписывается в практику организации

**Роль ЕА в управлении должна определяться ИТ-политикой.** В идеале, ИТ-политика должна определять роль функции ЕА в определении направлений, влияния на планы и утверждении проектных решений.

**ИТ-стратегические планы должны определяться дорожными картами ЕА и основываться на них.** ИТ-стратегические планы могут охватывать широкий круг проблем, в зависимости от того, что важно для организации, но при рассмотрении вопроса о согласовании с бизнес-факторами и планами ИТ-планировщики должны ссылаться на "будущие" состояния ЕА и соответствующие дорожные карты.

**Функция ЕА должна активно участвовать во всех руководящих органах.** ИТ-организации обычно внедряют руководящие органы, такие как руководящие комитеты ИТ по основным стратегическим приоритетам или операционные комитеты и комитеты по управлению программами, для отслеживания более локализованных решений. Руководителям групп ЕА следует использовать руководящий комитет по ИТ для утверждения программы ЕА, но они также должны решить, в какие руководящие советы входят. ИТ-директора должны признавать руководящие советы ЕА, такие как совет по обзору архитектуры, как расширение управления ИТ.

#### Эксперт по управлению портфелем проектов

Поскольку архитектура предприятия определяет прикладную и техническую архитектуры, команда ЕА может оценить, соответствуют ли предлагаемые решения проектов стандартам. Посредством планирования портфеля проектов команда может выявить взаимозависимости между проектами, которые могут повлиять на осуществимость и стоимость, или определить, есть ли возможности объединить проекты для создания лучших решений с меньшими затратами и за меньшее время. И наоборот, оценка портфолио предоставляет ЕА информацию о текущих потребностях бизнеса, которые учитывают потребности и приоритеты архитектуры. На этом уровне управления:

**Главные архитекторы входят в состав комитетов по управлению портфелем.** Комитет по управлению портфелем проектов рассматривает проектные инициативы, предложенные департаментами и ИТ, и принимает решения о приоритете проекта, масштабах и архитектуре высокоуровневого решения. Например, эти комитеты принимают решения о том, строить или покупать, будь то

масштаб проекта следует расширить или сузить, чтобы учесть другие инициативы и определить, когда следует инициировать проекты на основе имеющихся ресурсов.

Без участия архитектуры этот комитет может сделать немногим больше, чем распределять ресурсы на проекты, основанные на требованиях бизнеса. Участие архитектуры может помочь максимизировать ценность для организации за счет более продуманных, масштабируемых и упорядоченных инициатив.

**Процессы анализа PPM сочетают экономическое обоснование проекта с дорожными картами архитектуры.** Архитекторы могут использовать знания, полученные в ходе планирования и составления дорожных карт, для обеспечения понимания процесса принятия решений на сессиях по обзору портфолио. Как только организация осознает ценность вклада EA на этих встречах, бизнес-спонсоры проекта и руководители прикладных проектов будут искать членов команды EA перед сессиями по принятию решений для рационализации своих проектов и разрешения любых потенциальных конфликтов, которые могут препятствовать финансированию.

**Управление проектом Обеспечивает согласованность между EA и повседневными проектными решениями**

Управление проектами - это самый базовый уровень управления EA, который является общим для большинства программ EA. EA предоставляет подробное руководство по выбору технологии и передовым практикам проектирования, чтобы гарантировать соответствие проектов технологической стратегии и критериям качества. Группы EA используют два основных подхода к управлению: совместный и обзорный. В модели совместной работы архитектор решений обеспечивает руководство с самых ранних этапов проекта либо в качестве консультанта проектной группы, работающего полный или неполный рабочий день. В модели проверки совет по проверке архитектуры действует как контрольный процесс для утверждения хода перехода к следующему этапу проекта. EA участвует в управлении проектом в три этапа:

**До начала проектирования.** Архитекторы изучают требования и проверяют предположения относительно необходимости масштабируемости и интеграции с другими приложениями. Раннее вовлечение на этапе разработки требований позволяет им выявить шаблоны, которые могут ускорить процесс проектирования и исключить разовую работу по разработке. Поскольку организации внедряют сервис-ориентированную архитектуру (SOA), раннее вовлечение также позволит архитекторам определить, какие доступные сервисы могут быть использованы в проекте. Руководство на этом этапе чаще всего предоставляется с помощью модели совместного консультирования, хотя некоторые группы экспертов используют ранние "информационные обзоры", чтобы обеспечить возможность проведения мозгового штурма на ранней стадии с помощью советов по обзору архитектуры. Руководство на этой ранней стадии чрезвычайно эффективно и может устранить необходимость в "полицейском" характере проверок на более поздних этапах цикла разработки.

**До начала строительства.** Проверка ЭО в конце проектирования, как процесс перехода к стадии строительства, является наиболее распространенным типом управления ЭО. Команды EA, обычно созданные советом по обзору архитектуры, но иногда в рамках процесса совместной работы (особенно для проектов с низким уровнем воздействия), тщательно изучают проекты на предмет соответствия стандартам и лучших практик проектирования. Проверка определяет, соответствует ли конструкция качественным параметрам безопасности, производительности, надежности и ремонтопригодности. Этот тип управления проектом очень эффективен, но если это первое участие архитекторов в проекте, это придает управлению EA характер полицейских действий и может стать источником организационных конфликтов.

**До внедрения.** В ИТ-организациях с высокой степенью ориентации на процессы проекты пересматриваются повторно после завершения строительства, чтобы убедиться, что проект соответствует всем стандартам инфраструктуры и что он прошел тестирование должным образом. Это необычный контрольный пункт, и там, где он существует, EA участвует в процессе, а не управляет им.

**Управление обеспечивает обратную связь с архитектурой предприятия.**

Процессы управления EA повышают степень взаимодействия между архитекторами и лицами, принимающими бизнес-решения, ИТ-менеджментом, спонсорами проекта и руководителями групп разработки приложений. Они создают процессы обратной связи, которые гарантируют, что программа EA не просто диктует EA представление о том, каким должно быть будущее, но, скорее, постоянно учитывает текущие потребности и приоритеты, чтобы обеспечить значительную долю реальности в деятельности EA по планированию.

**Каждая организация адаптирует управление EA к своим потребностям**

Поскольку все фирмы разные, они по-разному подходят к управлению. В крупной организации, скорее всего, будет больше формализованных процессов и ролей, в то время как в небольшой организации особое внимание будет уделяться консультационным отношениям. Аналогичным образом, организации, использующей обширный аутсорсинг, потребуется подходить к управлению архитектурой иначе, чем к тому, при котором большая часть разработок осуществляется собственными силами, например, делая упор на документированные оценки и спецификации.

## УПРАВЛЕНИЕ - ЭТО НЕ ПОЛИЦЕЙСКАЯ ДЕЯТЕЛЬНОСТЬ, А РЕЗУЛЬТАТ

Организации, внедрившие успешные модели управления, получили поддержку руководства, а также широкую поддержку со стороны ИТ-специалистов, поскольку они эффективно донесли ценность EA до этой аудитории. Хотя ни одна организация не является бесконфликтной - и не должна стремиться к этому, - участники успешных процессов управления приветствуют вклад архитекторов и считают EA ценной и неотъемлемой частью планирования и развития. Чтобы процессы управления не отвлекали вашу организацию на непродуктивные конфликты, а вместо этого приближали вас к вашим целям:

**Постройте свой подход к управлению, начиная с управления ИТ.** Когда управление EA рассматривается организацией как отдельное от основных процессов управления, оно теряет свое влияние. Скорее, вам следует убедиться, что связь процессов управления EA с целями, планами и успехом организации в целом четко обозначена.

**Будьте инклюзивны в планировании и разработке ЭО.** Когда отдельные сотрудники участвовали в разработке плана, дорожной карты и артефактов EA, они, как правило, принимают на себя ответственность за цели EA и становятся частью решения. Лидеры мысли, оставшиеся в стороне, являются потенциальными противниками духа процессов управления EA.

**Интегрируйте EA с ИТ-планированием и расстановкой приоритетов.** ИТ-организации часто сталкиваются с трудностями в процессе планирования из-за объема коммерческих предложений и сложности оценки их последствий для ИТ-ресурсов и технологий. Группа EA должна предложить свои знания систем предприятия и свои навыки проектирования, чтобы помочь преобразовать эти предложения в проекты, которые наилучшим образом максимизируют выгоды для бизнеса и ИТ-возможности.

**Как можно раньше примите участие в управлении проектом.** Лучшее время для начала управления проектом - до принятия решений. Когда проекты пройдут путь от искорки в глазах спонсора проекта до значимого набора требований, попросите архитектора начать мозговой штурм решений с командой разработчиков.

### Подход 1: публикация документации по архитектуре

- Это подход к управлению по принципу "если вы создаете, то они придут".
- Документация по архитектуре становится доступной, и ожидается, что ИТ-сообщество просто подчинится ей.
- Хотя архитектурная документация может быть важной частью процессов управления, этот подход никогда не работает сам по себе. ИТ-специалисты не задействованы
- в каких-либо процессах, и влияние простой публикации документации по архитектуре обычно равно нулю, когда не существует процессов управления. Однако публикация документации является отправной точкой, на которую можно ссылаться на любом этапе для соблюдения стандартов. Это служит ориентиром на любых этапах проекта.

### Подход 2: Контроль процесса закупок ИТ

- Команда по закупкам, которая закупает ИТ-продукты и услуги, должна отчитываться внутри НЕЕ.
- Продукты, которые покупает эта команда, цикл закупок с помощью этих продуктов уникальны для НЕЕ. скорость изменений и связанная с этим ответственность
- Более того, благодаря контролю за закупками ИТ может стать инструментом, побуждающим людей покупать продукты, которые соответствуют архитектуре.

- Процесс закупок, который позволяет очень легко приобретать продукты, соответствующие архитектуре, и обременительная покупка нестандартных изделий способствует соблюдению стандартов. По крайней мере, исключается покупка нестандартной технологии из-за незнания стандартов. Привязка процессов закупок ИТ к стандартам архитектуры - ключевой способ институционализировать заботу об архитектуре предприятия в культуру организации.

#### **Подход 3: Созыв совета по обзору архитектуры**

- Советы по обзору архитектуры - это органы, которые регулярно собираются для рассмотрения архитектуры новых инициатив.
- Обзор архитектуры задуман как процесс отбора, который утверждает или отклоняет проекты на основе их соответствия установленной архитектуре и общим принципам проектирования.  
Это может быть чрезвычайно эффективно, когда процессы и методологии разработки
- систем и управления проектами широко используются, а анализ архитектуры включен в качестве стандартного этапа в эти процессы. В то время как немногие советы по рассмотрению архитектуры руководствуются железной хваткой, подразумеваемой их минимиными полномочиями
- по утверждению / отклонению, само существование процесса рассмотрения архитектуры может оказать существенное влияние на выбор технологии и разработку приложений.  
Недостатки этого метода управления включают потенциальную бюрократию при добавлении этапа проверки,
- трудность привлечения широкого участия в некоторых средах, отсутствие полномочий для изменения проектов и потенциальное отставание в проведении проверок в динамичных средах и возникающее в результате узкое место.

#### **Подход 4: Предоставление консультаций по архитектуре предприятия**

- Наиболее эффективным и наименее бюрократизированным процессом управления является использование внешних консультантов по архитектуре на ранних стадиях проекта для предоставления рекомендаций относительно выбора технологии и общей экспертизы проекта.
- В отличие от процесса контроля со стороны совета по обзору архитектуры, использование консультационной модели обеспечивает управление в форме упреждающего руководства по проектированию. Усвоив стандарты архитектуры, консультанты могут направлять разработчиков к разработке дизайна, соответствующего технологической стратегии.
- В то время как процесс консультирования может быть беспроигрышным как для архитектуры, так и для девелоперского сообщества.  
Этот подход может внести значительный вклад в оптимизацию подхода к управлению архитектурой

### **10.3 Совет по обзору**

Советы по обзору архитектуры собираются, чтобы утвердить или отклонить архитектуру / проекты проекта архитектуры

Обзоры архитектуры должны проводиться до того, как проектная группа завершит этап архитектуры и проектирования, и до того, как проект перейдет в фазу разработки / внедрения.

В дополнение к простому утверждению / отклонению, рекомендации по приведению ошибочной конструкции в соответствие с технологической стратегией также могут быть представлены в форме условных утверждений.

Членский состав наблюдательного совета должен охватывать необходимый спектр технологических знаний, но он должен также включать представителей любых подразделений департамента, которые, как ожидается, будут придерживаться архитектурных стандартов. В большинстве организаций забота о соблюдении архитектуры эффективно укоренилась в ИТ-культуре только тогда, когда существует сильное чувство сопричастности.

Ядро правления составляют члены центральной архитектурной группы, при этом глава группы выступает в качестве председателя и лица, принимающего окончательные решения. Процесс должен включать обсуждение проекта и голосование по утверждению; однако утверждение не должно быть вопросом простого большинства. Любое противоречивое мнение должно быть разрешено, а не отброшено в сторону, при этом председатель принимает решение об эскалации конфликтов или переводе их в автономный режим. Наблюдательный совет - это не место для бесконечных дискуссий о тонкостях дизайна; это скорее простой процесс презентации, обсуждения и голосования, на каждый проект отводится максимум полчаса. Любая проверка, которая не укладывается в эти временные рамки, должна рассматриваться на онлайн-собраниях.

Среди участников проекта на заседаниях совета по обзору архитектуры должны быть бизнес-спонсор проекта и разработчик приложений. Постоянные члены совета по обзору архитектуры должны включать основных членов центральной архитектурной группы и представителей архитектуры из организационных подразделений инфраструктуры и развития.

Членский состав наблюдательного совета должен охватывать необходимый спектр технологических знаний, но он должен также включать представителей любой политической организации, от которой ожидается соблюдение архитектурных стандартов. В большинстве организаций забота о соблюдении архитектуры эффективно укоренилась в ИТ-культуре только тогда, когда существует сильное чувство сопричастности.

Ядро правления составляют члены центральной архитектурной группы, при этом глава группы выступает в качестве председателя и лица, принимающего окончательные решения. Процесс должен включать обсуждение проекта и голосование по утверждению; однако утверждение не должно быть вопросом простого большинства. Любое противоречивое мнение должно быть разрешено, а не отброшено в сторону, при этом председатель принимает решение об эскалации конфликтов или переводе их в автономный режим. Наблюдательный совет - это не место для бесконечных дискуссий о тонкостях дизайна; это скорее простой процесс презентации, обсуждения и голосования, на каждый проект отводится максимум полчаса. Любой обзор, который не может уложиться в эти временные рамки, должен рассматриваться на онлайн-встречах.

Сроки проведения проверок (то есть окончание этапа проектирования) могут быть проблематичными - после того, как проектирование завершено, может возникнуть значительное давление со стороны бизнеса, вынуждающее приступить к строительству в соответствии с графиками и бюджетами, а отклонение или модификация советом по проверке архитектуры может рассматриваться как бюрократическое препятствие, которое необходимо обойти или убрать с дороги. Такие конфликты проверяют авторитет правления, и частые сбои в эффективном отклонении проектов могут привести к тому, что правление будет выглядеть как бесполезный штампованный процесс. Обзор проекта на ранних стадиях проектирования может быть полезен, но чаще всего значительный объем деталей недоступен, и совет по надзору за архитектурой не должен выдавать разрешения на незавершенные проекты. Этот фундаментальный конфликт между потребностью в завершенном проекте для рассмотрения и утверждения и нежеланием бизнес-спонсоров откладывать проекты, за отклонение которых совет по обзору архитектуры голосует, является главной трудностью совета по обзору архитектуры как процесса управления. Однако советы по обзору архитектуры могут быть чрезвычайно эффективными, когда они являются частью комплексной программы управления, которая включает активную поддержку ИТ-директоров, коммуникационную программу, способствующую осознанию ценности архитектуры на низовом уровне и архитектурный консалтинг.

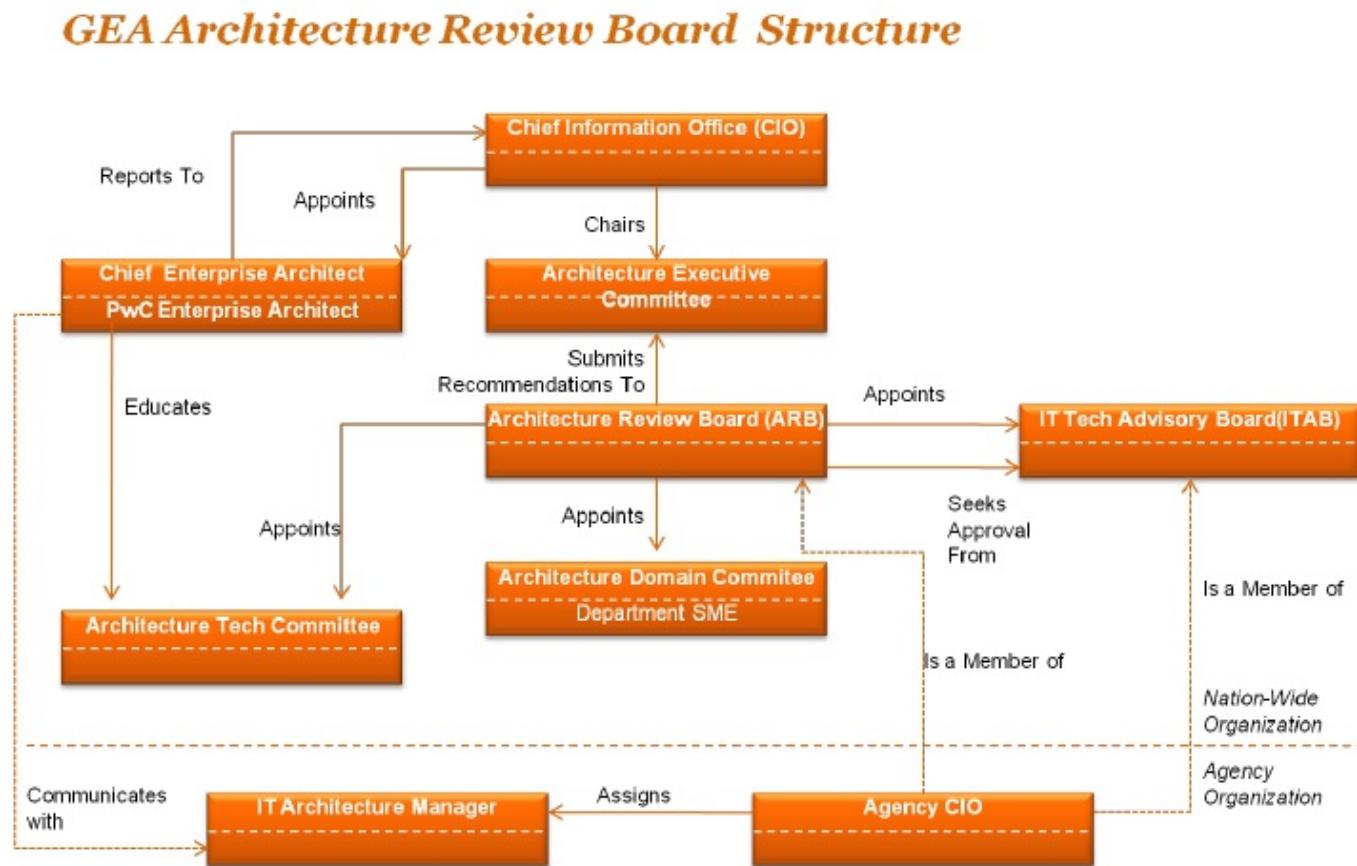
Финансирование этого процесса управления обычно осуществляется в форме "корпоративного налога" на время центральных архитекторов и готовность инфраструктурных и девелоперских групп финансировать должность архитектора для участия в деятельности, связанной с архитектурой.

Плюсы		Минусы
getDesigns рассмотрено практиков.	высоко	квалифицированный ИТ-архитектура рассмотрение происходит в конце проекта, приводит к доработке или отказу изменять дизайн.
Осознание важности архитектуры повышается в ИТ-сообществе.		Неспособность обеспечить соблюдение требований из-за давления бизнеса с целью соблюдения графика подрывает усилия по созданию архитектуры и деморализует участников.
ИТ-организация обеспечивает повышенное соответствие стандартам.		Перегруженная плата может создать бюрократическое узкое место в процессе внедрения, нанося ущерб архитектурным усилиям.
ИТ-организация получает повышенную осведомленность о веских бизнес-причинах несоблюдения и необходимости расширения стандартов архитектуры.		

## 10.4 Жизненный цикл управления архитектурой предприятия.

### 10.4.1 Структура управления архитектурой предприятия

Примерная предлагаемая модель управления GEA представлена ниже -

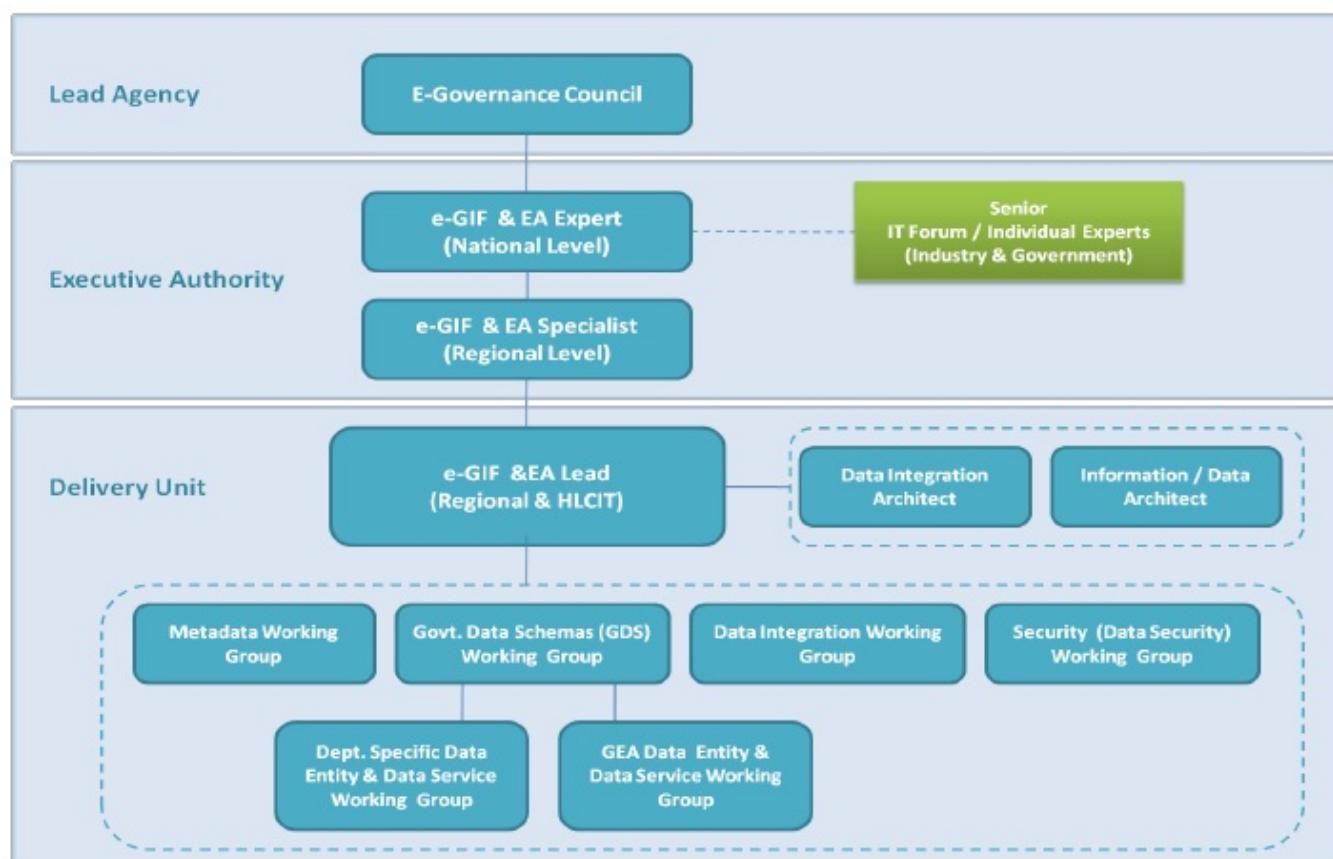


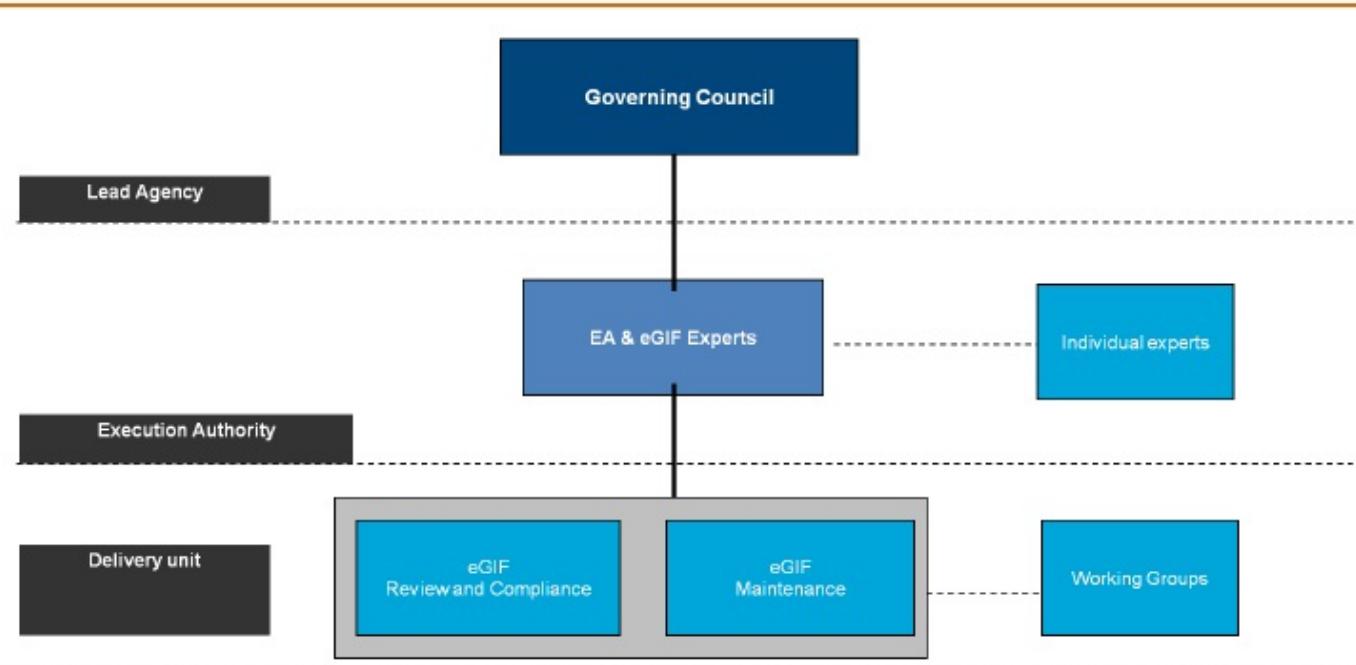
Предложенная выше структура управления является ориентировочной. Эта структура будет пересмотрена и доработана после обсуждения с HLCIT, РМО и другими соответствующими органами и будет представлена в качестве добавления к этому отчету

Функции	Описания	Отображение правительства SEA Mapping	
Директор по информации (CIO)	Поддерживает усилия в области архитектуры, продвигает ценность архитектуры, обеспечивает успех архитектуры, выделяет соответствующие ресурсы и управляет принципами архитектуры. Утверждает ИТ-проекты для крупных бюджетных проектов и поддерживает процесс составления бюджета и выделения средств от имени других агентств.		
Архитектура Исполнительный Комитет (AEC)	Утверждает варианты архитектуры, проверяет планы проекта, стратегию управления рисками на соответствие архитектуре. Внедряет процессы управления; обучает фасилитаторов и пользователей; управляет целями и показателями эффективности, управляет планом внедрения ; управляет содержанием архитектуры; администрирует проверки соответствия требованиям; разрабатывает шаблоны доменов; и администрирует ARC.		
Главный архитектор	Представляет рекомендации по архитектуре в AEC, рассматривает		
Обзор архитектуры Архитектурные изменения, отклонение Комитета (ARC), создание	архитектура запросы на управление обзоры процессами; назначает фасилитаторов и архитектурные комитеты и председателей доменов.		
Архитектурный домен Комитеты (ADC)	Рекомендует стандарты архитектуры, обеспечивает консультирование агентств по предметной области и предоставление технической помощи по вопросам, касающимся архитектуры.		
Технический комитет по архитектуре (ATC)	Обучайте доменные комитеты, проводите сессии по предметной области, гарантируйте соблюдение методологии, обеспечивайте согласованный корпоративный взгляд, добивайтесь консенсуса членов ADC, выступайте в качестве экспертов по методологии, и управляйте специальными проектами.		
Консультативный совет по информационным технологиям (ITAB)	Этот совет директоров состоит из ИТ-директоров уровня департамента и / или ИТ директоров. Реализует стратегический план и разрабатывает ИТ-стратегии. Имеет решающее значение для одобрения инициатив СИО . Выполняет функции ключевого контактного лица с заинтересованными сторонами проекта. Укомплектовывает многие из комитетов по политике и стандартам.		

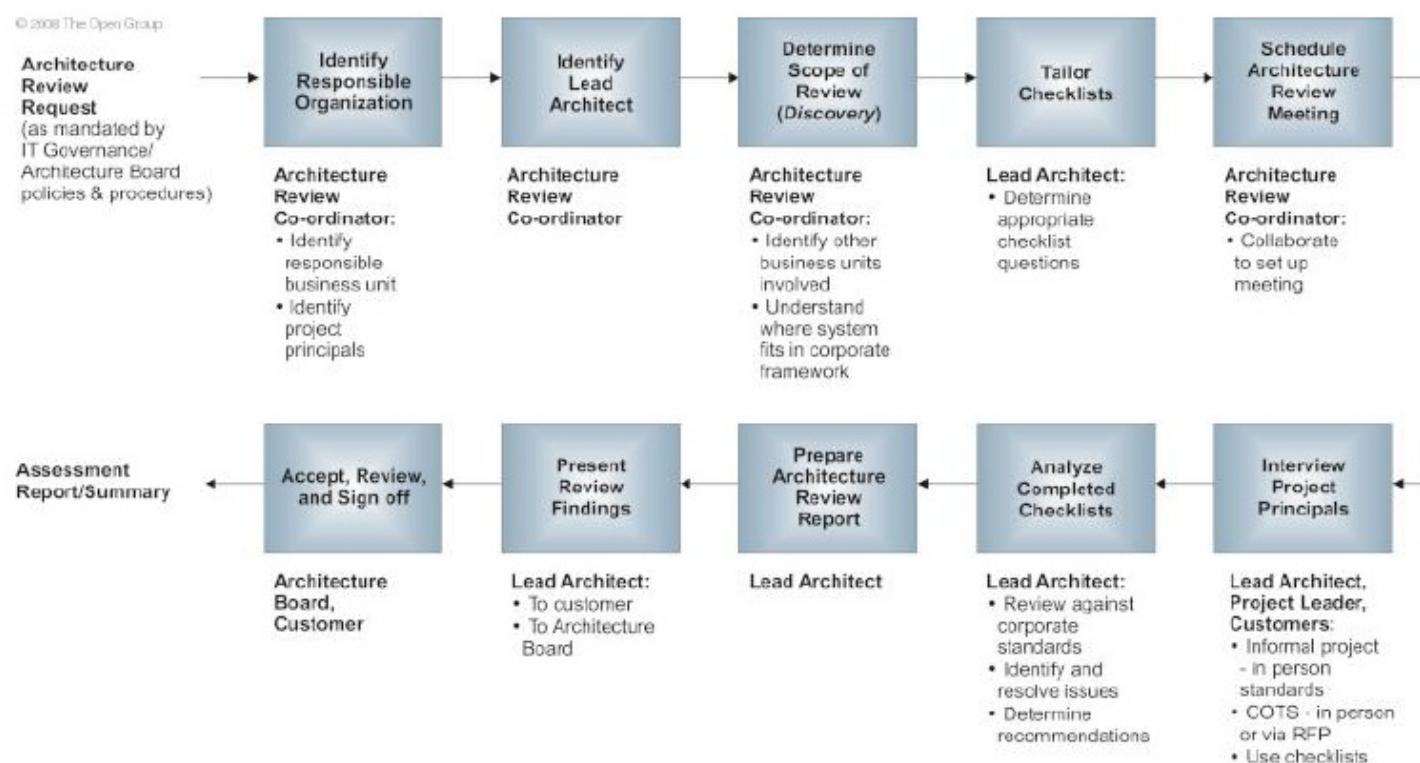
Функции	Описания	Карта правительства	Карта GEA
Менеджер по ИТ-архитектуре	<p>Устанавливает и управляет процессом соответствия требованиям департамента; взаимодействует с разработчиками, пользователями и mgers и обучает их;</p> <p>Устанавливает цели архитектуры и измерения; управляет базой данных по архитектуре департамента; управляет планом внедрения архитектуры ; обеспечивает соблюдение методологии; и выступает в качестве потенциального члена ATC.</p>	по	
Комитет по обзору архитектуры (ARC)	<p>Представляет рекомендации по архитектуре в AEC, рассматривает Архитектурные изменения, Отзывы Запросы для отклонения, установление управление архитектурой обрабатывает; назначает фасилитаторов и комитеты и председателей домена по архитектуре .</p>		
ИТ-директор агентства	Владеет архитектурой на уровне отдела.		

#### 10.4.2 Негативное управление





#### 10.4.3 Процесс проверки соответствия архитектуры

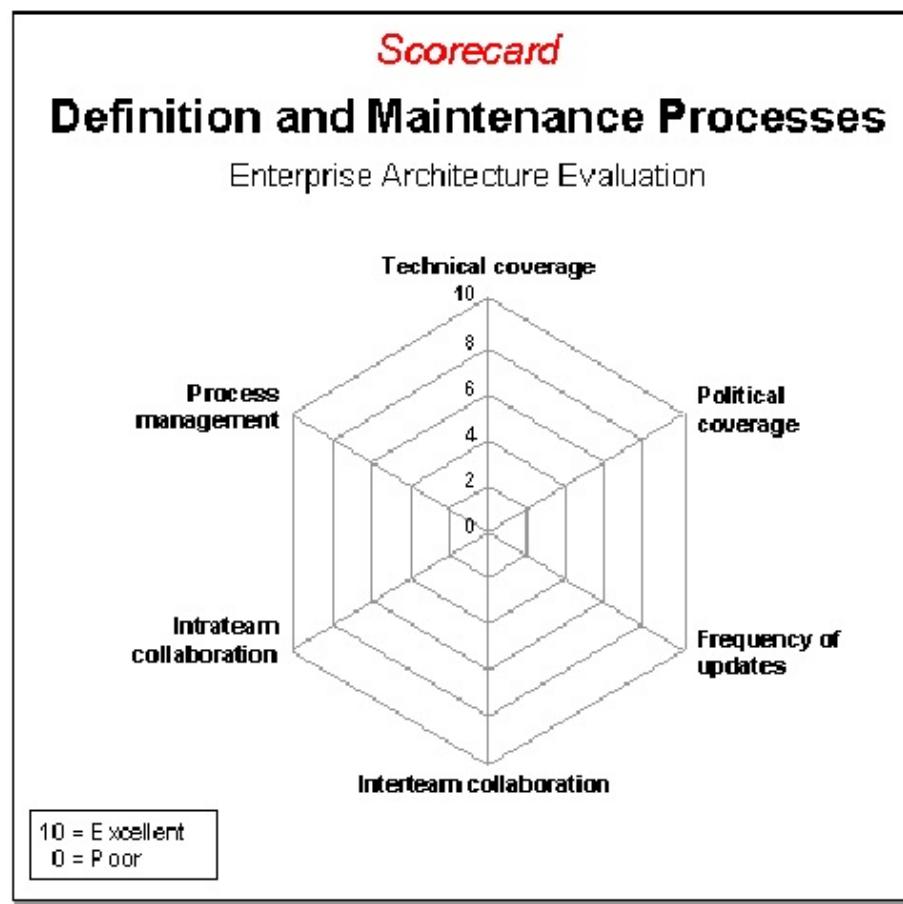


#### 10.4.4 Соответствие и оценка GEA

Оценка: процессы определения и сопровождения

- Технический охват
- Политический охват

- Частота обновлений
- Сотрудничество между командами
- Сотрудничество внутри компании
- Управление процессами



Source: Giga Information Group

Figure 1

#### 10.4.4.1

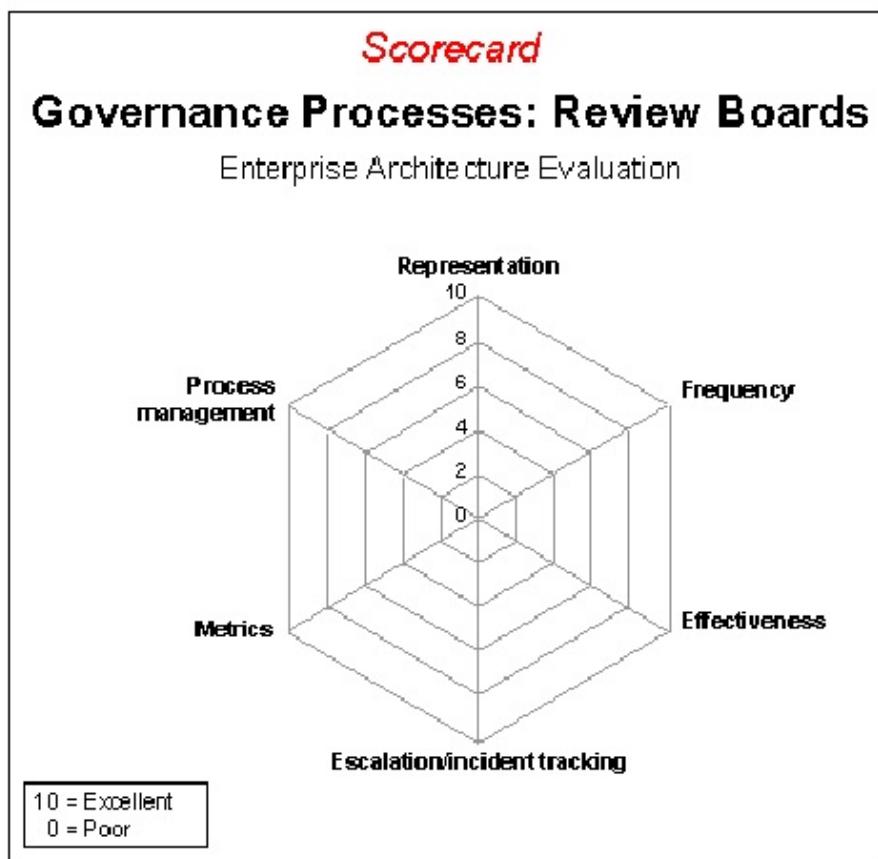
#### Зрелость оценки

##### Процессы управления: Наблюдательные советы

Использование советов по обзору архитектуры является распространенным подходом к управлению архитектурой. Они могут быть эффективными в предоставлении широкой и высококвалифицированной аудитории для обзоров дизайна и в качестве средства передача архитектурной информации о проектах с высокой отдачей. Однако некорректные реализации могут расстраивать архитекторов и заинтересованных сторон в архитектуре, а также множество факторов, влияющих на потенциал эффективности советов по проверке, включая состав совета, частоту проверок и внедрение механизмов отслеживания инцидентов.

- Представительство
- Частота
- Эффективность
- Отслеживание эскалации / инцидентов
- Показатели

- Управление процессами



Source: Giga Information Group

Figure 2

### Процессы управления: консалтинг

Хотя внутренний консалтинг по архитектуре обычно рассматривается как средство обмена техническим опытом, он также может быть очень мощным механизмом управления архитектурой, а гибкий режим консультирования позволяет избежать основных трудностей, присущих совету по рассмотрению архитектуры как механизму управления, а именно своевременности и навязывания бюрократии и восприятия архитектуры как полицейского действия. Однако хорошо предоставлять консультации сложно; необходимы отличные технические навыки и "мягкие" навыки, что приводит к нехватке подходящих специалистов, а также к управлению консалтинговыми ресурсами в широком масштабе

- Всесторонность
- Роли/организационные вопросы
- Хронометраж
- Эффективность
- Управление знаниями
- Показатели
- Управление процессами

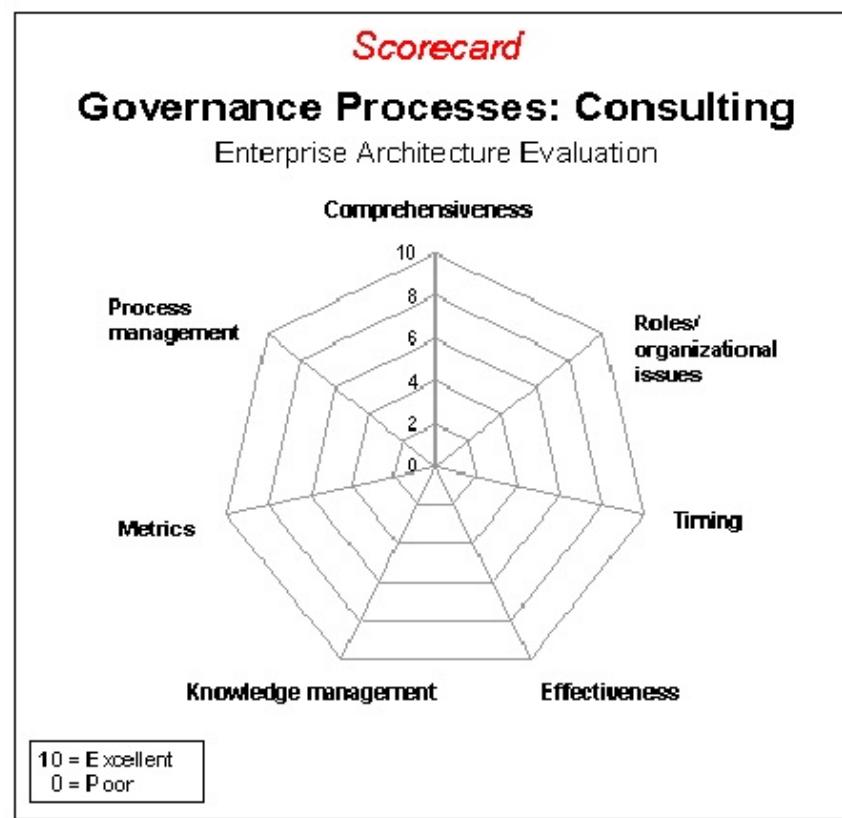
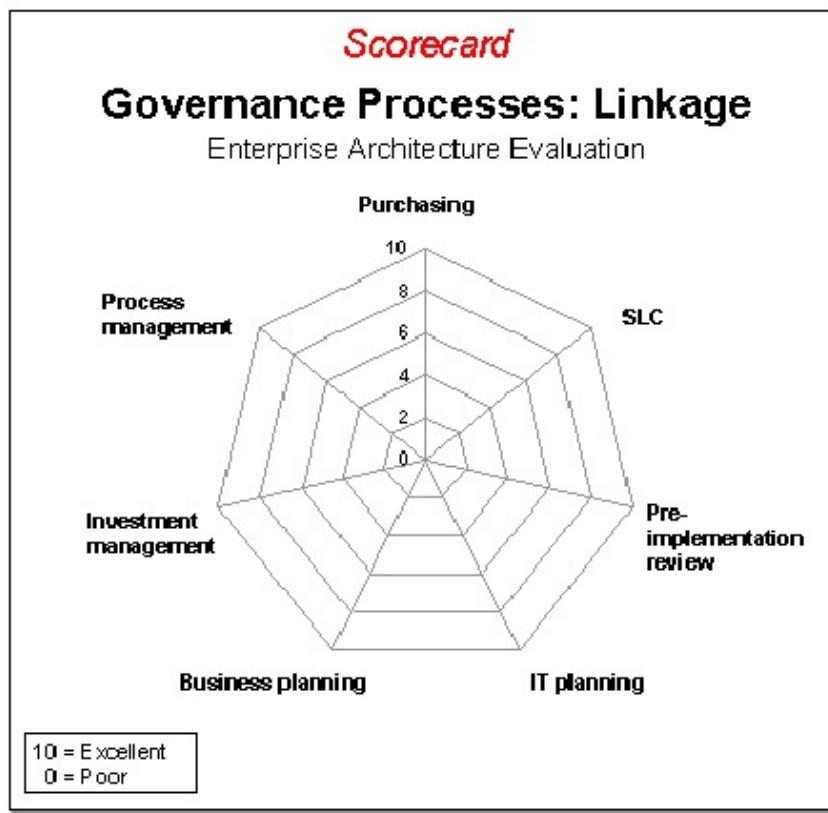


Figure 3

#### Процессы управления: Взаимосвязь

Увязка процессов архитектуры с другими ключевыми ИТ- и бизнес-процессами имеет решающее значение для эффективного управления архитектурой. Например, привязка стандартов архитектуры к процессу закупок может исключить непреднамеренные закупки нестандартных технологий и препятствовать сознательным усилиям по приобретению нестандартных компонентов. Привязка к процессам жизненного цикла разработки системы может иметь решающее значение для оказания влияния на деятельность по разработке. И необходимость привязки к процессам планирования должна быть очевидна каждому, кто пытался поддерживать архитектуру в синхронизации с бизнес-требованиями.

- Покупка
- Жизненный цикл системы (SLC)
- Предварительный обзор внедрения
- ИТ-планирование
- Бизнес-планирование
- Управление инвестициями
- Управление процессами



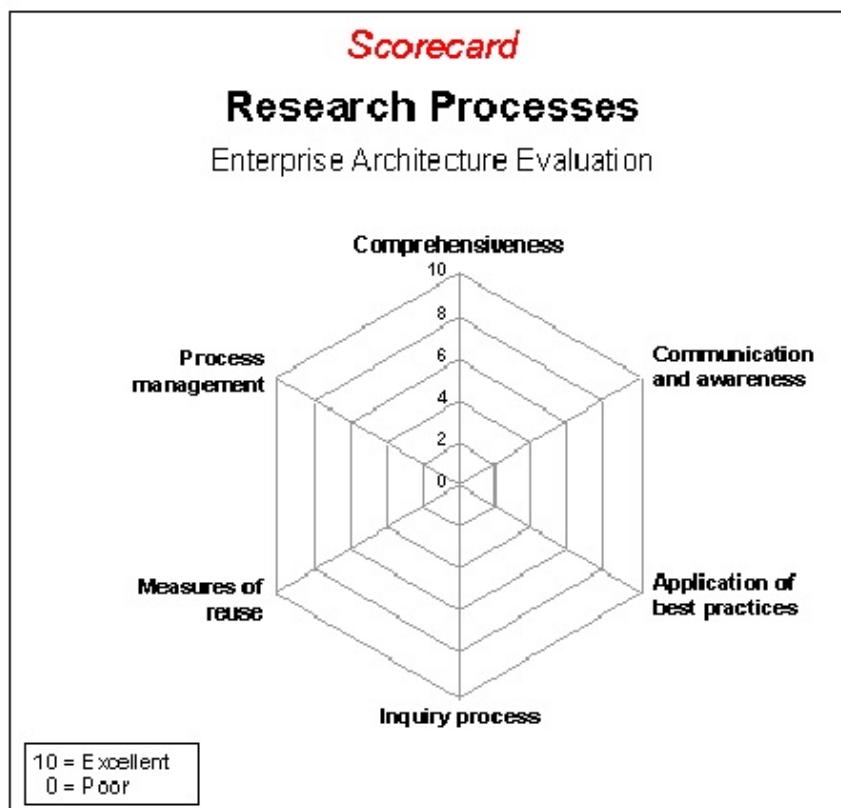
Source: Giga Information Group

Figure 4

### Процессы управления: Взаимосвязь

Каждая архитектурная группа участвует в исследовательских процессах, независимо от того, считают ли они свои процессы формальными конструкциями или нет. Степень, в которой эти процессы структурированы для эффективного использования ресурсов, затраченных на исследования, значительно варьируется от организации к организации. Эти критерии оценивают способность архитектурной группы использовать свои исследовательские процессы для общего улучшения предприятия.

- Комплексность.
- Коммуникация и осведомленность.
- Применение передовых практик.
- Процесс запроса.
- Меры повторного использования.
- Управление процессами.



Source: Giga Information Group

Figure 5

## 10.4.4.2

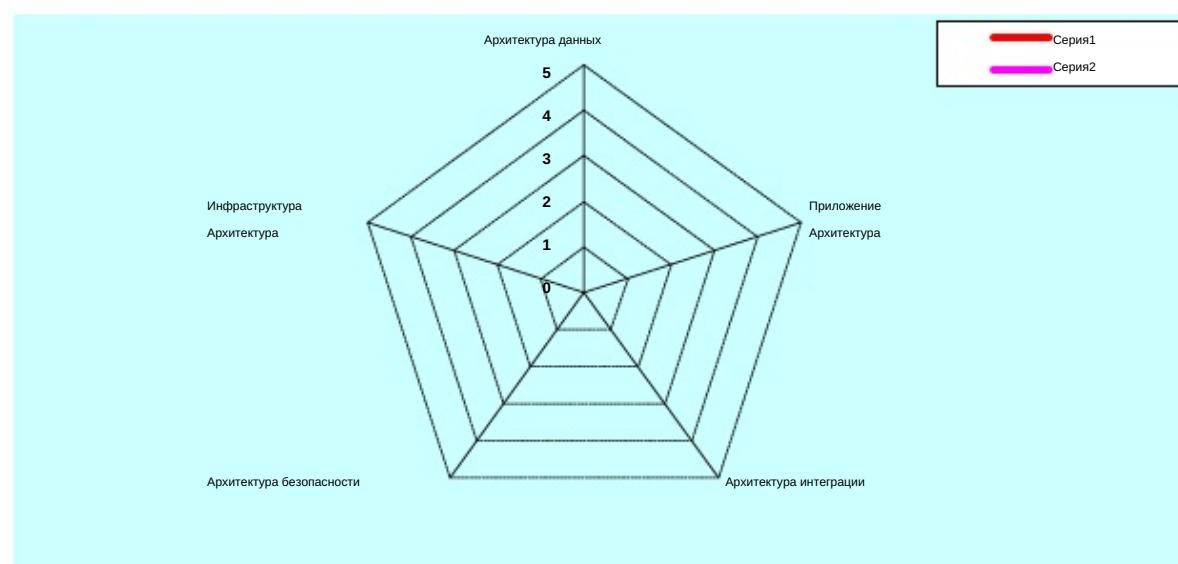
## Контрольный список для оценки архитектуры

ID	Раздел	Значимость для измененного проекта (Г/П)?	Выберите ответ	Дополнительные подробности / Комментарии	Оценка
1.	<b>Архитектура данных</b>				
	система за a01a Отвечает ли управление основными данными?				
	пользователю в a01b Доступны ли данные своевременно				
a01c	Как вводятся и проверяются данные?				
a01d	Каким образом поддерживается или обеспечивается ссылочная целостность посредством процесса обновления / копирования данных?				
	архитектура данных a01e модель этой системы?				
a01f	Является стратегией хранения данных, архивирования & определено и реализовано удаление?				
владельцы бизнеса a01g	Существуют ли отдельные для каждой ключевой категории данных?				
существующими a01h	Учитывалось ли повторное использование существующими				

ID	Раздел	Значимость для измененного проекта (Г / П)?	Выберите Ответ	Дополнительные Подробности Комментарии	/ Оценка
	рассмотрение этого проекта?				
<b>Архитектура</b>					
<b>приложения 2.</b>					
	Какие типы методов доступа a02a (технические) поддерживаются этим приложением?				
	Насколько гибким является приложение для a02b интерфейса сторонних производителей				
	системы?				
a02c	Как это реализовано?	База данных	доступ		
	Как работает параллелизм базы данных и транзакция a02d		Руководство		
	реализовано?				
	Как устроены бизнес-правила и логика a02e				
	определенено в этом приложении?				
a02f	Приложение что предоставлено?	ведение журнала	является		
a02g	Какой уровень усилий потребовался бы для мигрировать этот для приложения на другой платформе?				
a02h	Каковы исключения / ошибки a02h, управляемые и сообщаемые пользователям в этом приложении?				
a02i	Как выполняется проверка данных a02i для онлайн-экранов?				
(например,	Был ли доступен AAA) a02j разработано в приложении?				
3.	<b>Архитектура интеграции</b>				
a03a	Какие интерфейсы (API) для прикладного программирования, поддерживаемые применение (Примечание: некоторые этим API с более низкой оценкой, могут подходить в обстоятельствах, например, для производительности)?		быть каким-то		
	Сам стандартный / существующий BI / a03b средства создания отчетов имеют доступ к этой системе? Готово ли это				
приложение для a03c	Единый вход?				

ID	Раздел	Значимость для измененного проекта (Г / П)?	Выберите Ответ	Дополнительные Подробности / Комментарии	Оценка
a03d	Разрешен или возможен ли прямой внешний доступ к исходным системным данным core a03d ?				
a03e	Использует ли это приложение четко определенные определения XML-схемы (XSD)?				
a03f	Какие протоколы поддерживаются a03f это приложение?				
a03g	Взаимодействует ли это приложение с a03g с промежуточным программным обеспечением (например, MQSeries, ESB, EAI, TP monitor)?				
a03h	Как это приложение поддерживает a03h основные данные предприятия?				
a03i	Разрабатываются ли интерфейсы один раз для функции / элемента данных или приложения "точка- a03i" с помощью основание для подачи заявления?				
4.	<b>Архитектура безопасности</b>				
a04a	Работает ли это приложение имеет модель аутентификации и авторизации в этом				
a04b	приложении Включен ли аудит в приложении				
a04c	Определены ли все данные по классификации безопасности a04c и для комбинация				
a04d	данных Имеет обмен всеми ненормированными данными с a04d организации и отдельные лица, использующие общедоступные сети, надежно зашифрованы	внешние			
a04e	управление безопасностью и идентичность реализованный отдельно от бизнес-процесса	имеет был			
a04f	, проходит ли он независимую тестирование на проникновение				
5.	<b>Архитектура инфраструктуры</b>				
a05a	развернуто защищенным в окружающая среда?				
a05b	Тестируировалось ли это приложение на a05b аналогичная установка во время предварительной подготовки				

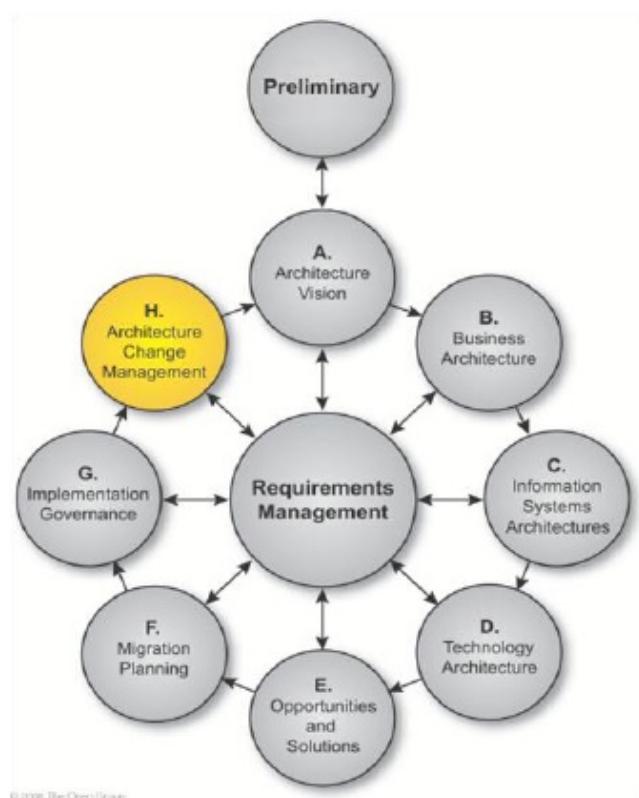
ID	Раздел	Значимость для измененного проекта (Г / П)?	Выберите Ответ	Дополнительные Подробности / Оценка Комментарии
	производственные испытания?			
	Были ли задокументированы все допущения относительно а05c, на которых основаны обязательства по исполнению ?			
a05d	тот Имеет адекватно размер производительность / пропускная способность, пользователи и т.д.)?	бывшее в употреблении (хранилище,		
	Является ли это приложение производительным а05e тестировался на масштабируемость? Возможно ли развертывание			
	этого приложения в распределенной среде, допускающей а05f масштабируемое оборудование, балансировка нагрузки, п-уровни?			
a05g	потенциально Есть узкие места / возникли проблемы определенны и решены? Есть экономически	с производительностью		
	эффективные пути внесены улучшения в производительность для каких-либо проблемных областей?	для		
момент a05i	Работает ли приложение в данный есть проблемы с производительностью? Каков измеренный максимальный объем			
a05j	(транзакции, пользователи), который может поддерживать это приложение?			
	Удовлетворяет ли это приложение заявленному а05k требованиям к доступности?			
a05l	Включает ли эта система аварийного восстановления?	включить		
	Как защищены данные для передачи а05m по сети			



## **11. Фаза Н TOGAF ADM - Управление изменениями архитектуры**

## Фаза Н: Архитектура 11.

### Управление изменениями



#### Обзор этапа

Цель процесса управления изменениями архитектуры - гарантировать, что архитектура достигнет своей первоначальной целевой ценности для бизнеса. Это включает в себя управление изменениями в архитектуре согласованным и продуманным способом для создания и поддержки внедренной корпоративной архитектуры как динамической архитектуры. Этот процесс обычно предусматривает постоянный мониторинг таких вещей, как новые разработки в области технологий и изменения в бизнес-среде, а также для определения того, следует ли формально инициировать новый цикл эволюции архитектуры

© 2008 The Open Group

#### 11.1 Запрос на архитектурные работы

Контракт на управление архитектурой между архитектурной функцией и бизнес-пользователями предприятия

#### 11.2 Изменения структуры и принципов архитектуры

##### Подход

Определите, оправдан ли запрос на изменение

Запуск нового цикла метода разработки архитектуры (ADM)

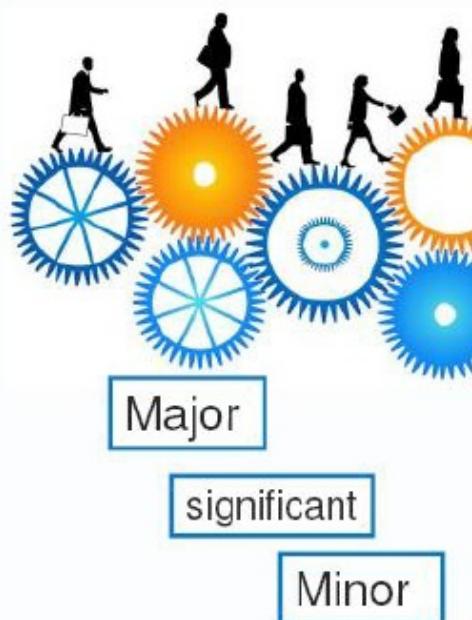
Просто обновление архитектуры

Важно избегать "ползучей элегантности", и руководящий орган должен продолжать искать изменения, которые напрямую связаны с ценностью бизнеса. В отчете о соответствии архитектуры должно быть указано, соответствует ли изменение текущему архитектуре.

Если она не соответствует требованиям, может быть предоставлено исключение. Если изменение оказывает значительное влияние на архитектуру, то должна быть разработана стратегия управления его воздействием. Определены движущие силы изменений

Существует три способа изменения существующей инфраструктуры, которые должны быть интегрированы:

Стратегические изменения, направленные сверху вниз для улучшения или создания новых возможностей (капитала) [Реорганизация]  
Изменение]  
Изменения снизу вверх для исправления или расширения возможностей  
(эксплуатации) [Управление операциями] [Инфраструктурное изменение] Опыт  
работы с ранее реализованными проектами увеличивается в процессе управления операциями,  
но все еще выполняется текущими проектами [Упрощение процесса]



### 11.3 Процесс управления изменениями архитектуры

Чтобы определить, является ли изменение упрощением, приращением или реорганизацией архитектуры, выполняются следующие действия:

- Регистрация всех событий, которые могут повлиять на архитектуру,
- Распределение ресурсов и управление ими для задач архитектуры
- Процесс или роль, ответственная за ресурсы архитектуры, должна произвести оценку того, что должно быть сделано Оценка воздействий

#### Движущие силы изменений

Бизнес-движущие силы изменений архитектуры, включая:

Развитие обычного бизнеса Исключения для бизнеса  
Бизнес-инновации  
Инновации в бизнес-технологиях  
Стратегические изменения

Часто приводит к полной (или частичной) перестройке архитектуры

Связанные с технологией драйверы для запросов на изменение архитектуры включают, например.:

Отчеты о новых технологиях  
Снижение затрат на управление активами, отказ от технологий, Инициативы по разработке стандартов  
Обычно управляемые с помощью процессов управления изменениями и архитектуры предприятия . процессы

#### Техническое обслуживание или управление изменениями

Для определения масштабов изменений хорошим практическим правилом является следующее::

Если изменение затрагивает двух или более заинтересованных сторон, то, вероятно, потребуется редизайн архитектуры и

поступление в АРМ  
затрагивает только одну заинтересованную сторону, то с большей вероятностью она будет кандидатом на изменение управления Если изменение может быть разрешено в соответствии с разрешением, то с большей вероятностью она будет кандидатом на изменение руководство

Если влияние является значительным для

бизнес-стратегии Может возникнуть необходимость переделать всю При появлении новой технологии или стандартов,

архитектуру предприятия

Может возникнуть необходимость обновить технологическую архитектуру, но не все предприятия

Архитектура - таким образом, постепенное изменение,

если изменение происходит на уровне инфраструктуры

Например, десять систем сокращены или заменены на одну систему - это может не изменить архитектуру

выше физического уровня, но это изменит базовое описание Технологической архитектуры

Это было бы упрощенным изменением, осуществляемым с помощью методов управления изменениями

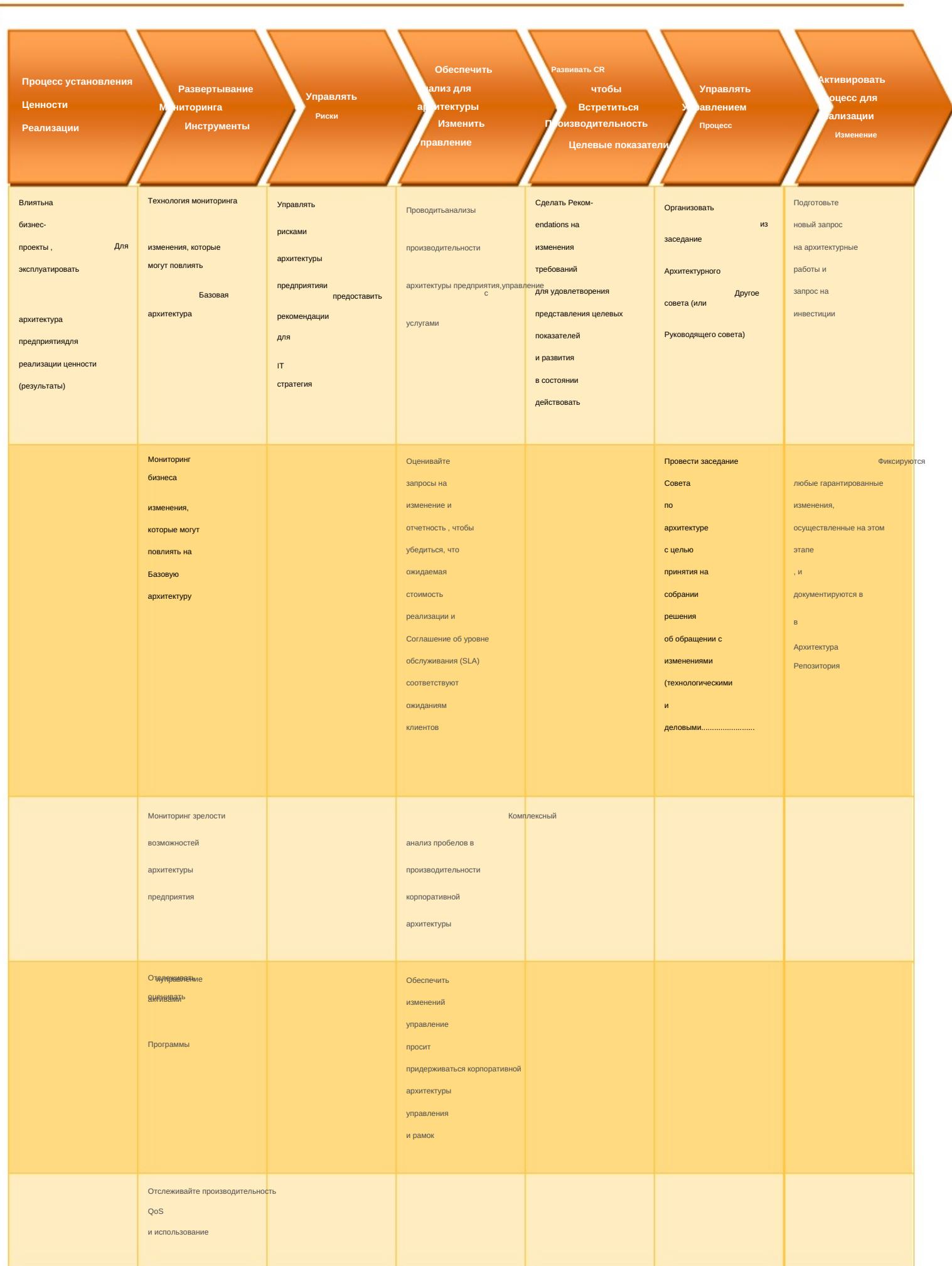
#### Архитектурный совет и Запросы на изменения

Архитектурный совет оценивает и утверждает Запросы на изменения (RFC)

Задача, стоящая перед Советом по архитектуре при работе с RFC, состоит в том, чтобы определить, должен ли он быть

одобрение проекта в переходной архитектуре архитектуре управления изменениями также может проблема иметь место случай, когда инновационное решение или RFC приводят к изменению архитектуры

#### 11.4 Процесс внедрения изменений



	Определять и отслеживать требования к непрерывности бизнеса						
--	--	--	--	--	--	--	--

## 11.5 Развёртывание инструментов мониторинга

Инструментами мониторинга являются коммерчески доступные продукты COTS, которые помогают поддерживать хранилище всех документов, относящихся к ADM, на основе TOGAF. Это позволяет проследить любой принцип от предварительных этапов до его реализации.

## 12. Аннексия

## 12. Аннексия

### 12.1 Типичный пример решения для шлюза электронных платежей

Решение для шлюза электронных платежей обычно предлагает следующие базовые функциональные возможности:

1. Платежный шлюз через Интернет - правительство Непала сможет получать различные платежи с веб-сайта электронного управления. Способами оплаты могут быть кредитная карта, дебетовая карта, сетевой банкинг и т.д.

В зависимости от услуг, предлагаемых поставщиком решения для шлюза электронных платежей 2. Прямая оплата - это средство, которое предоставит правительству Непала возможность принимать онлайн-платежи от своих граждан, которые также являются владельцами счетов в банках, одобренных правительством, и любых других банковских счетов, владельцев банковских паролей Net для совершения онлайн-платежей. 3. Система дебетовых электронных расчетов (ECS) - механизм ECS поможет гражданам по всему Непалу получить счет в любом банке / филиале, который является участником клиринга ECS. Поставщик услуг ePayment gateway (банк) выступит в качестве банка-спонсора для внедрения дебетовых ECS для приема платежей от граждан от имени правительства.

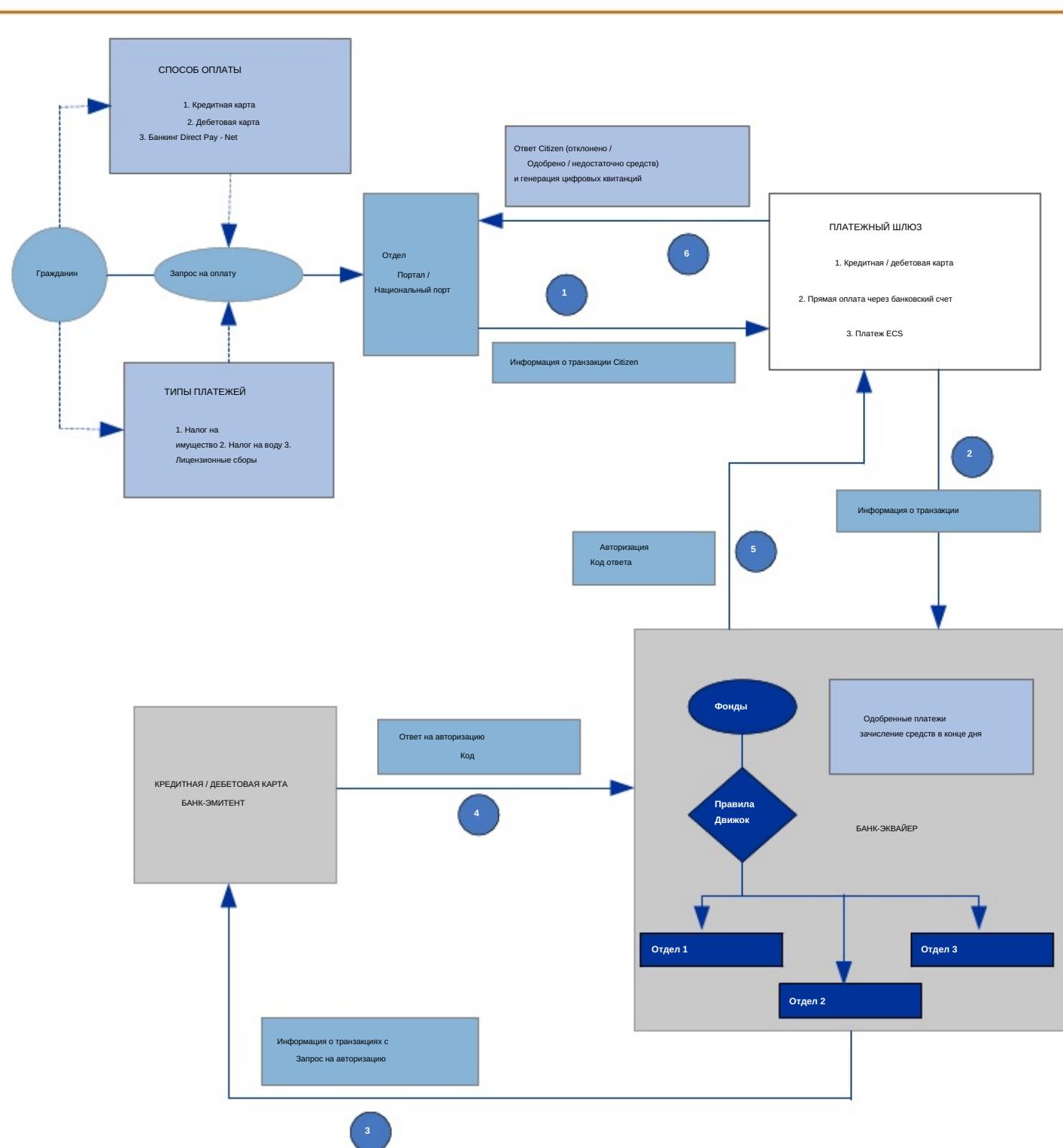
Идеальное решение платежного шлюза должно быть реализовано на основе следующих критериев:

• Аутентификация сторон, участвующих в транзакции  
• Безопасно перенаправлять сообщения между сторонами для авторизации и урегулирования транзакции  
• Обеспечивать целостность и конфиденциальность всех сообщений  
• Оказывать административную поддержку вовлеченным сторонам

Типичный операционный процесс для получения платежей через интернет-портал показан ниже -

1. Гражданин посещает портал государственного ведомства или национальный портал. Он отправляет запрос на электронную услугу и выбирает вариант онлайн-оплаты, если требуется платежная транзакция. Веб-сервер продавца получает сообщение и отправляет цифровой заказ на платежный шлюз по защищенной ссылке. Цифровой заказ содержит идентификатор продавца, подпись, сумму и обратный URL-адрес. Платежный шлюз проверяет продавца.
2. Затем он предоставляет гражданину экран вариантов оплаты по защищенной ссылке. 4. Гражданин предоставляет свою платежную информацию. Информация передается на платежный шлюз по безопасная ссылка.
5. Затем платежный шлюз передает эту информацию банку-эквайеру. Банк-эквайер проверяет лимиты продавца, а затем передает сообщение в банк-эмитент для авторизации платежа. Банк-эмитент авторизует платеж и передает подтверждение обратно на платежный шлюз через банк-эквайер.
6. Платежный шлюз отправляет цифровые квитанции в департамент и гражданину.

Весь процесс занимает несколько секунд. Платежный шлюз гарантирует, что платежная информация гражданина не будет передана продавцу. Он также гарантирует, что информация гражданина не будет скомпрометирована ни в какой момент. Это также позволяет банку-эквайеру верифицировать продавца.



[pwc.com/india](http://pwc.com/india)