Guidelines for IT Development Projects

هيئة المعلومات والحكومة الإلكترونية
Information & eGovernment Authority

Governance & Enterprise Architecture Directorate

Version 0.2 | 14th June 2021

Contents

Introduction

This document provides a set of guidelines and best practices for government entities to facilitate successful management and implementation of System and Application Development Projects.

The Guidelines

1.1 Project Governance

1.1.1. Government entities should form Project Steering Committee for each project with representatives from both business and IT.

1.2 Project Management

1.2.1 Government entities should utilize PMO Toolkit provided by iGA to facilitate project management activities.

1.3 Requirements Analysis

1.3.1 Development projects must include an initial phase for detailed Requirements Analysis and Business Process Reengineering (BPR) where the outcomes are reviewed and approved by the Project Steering Committee before the implementation phase.

1.3.2 The BPR exercise must perform a detailed assessment of the business and IT solution requirements. The BPR exercise is required to carry out an exhaustive requirement gathering in coordination with the entity for understanding the detailed requirements. During requirement gathering stage, entities should develop and follow standardized templates for capturing requirements and system documentation, modify and enhance the Business Requirements Document (BRD), prepare a Software Requirement Specification (SRS) based on the BRD document, and obtain a sign-off from the steering committee (no additional cost shall be paid for such changes till the SRS approval stage).

1.4 Development

1.4.1 iGA recommends that whenever citizen authentication is required must go through eKey (National Authentication Framework).

1.4.2 iGA recommends that whenever integration with external stakeholder is required must go through the NGI (National Gateway Infrastructure) to ensure reusability of integration components and services across the government.

1.4.3 The entity needs to consider the usage of managed database services such as RDS as a service from AWS (recommended databases include PostgreSQL, Enterprise MYSQL, or MangoDB).

1.4.4 iGA highly recommends that the solution must be developed and tested on using DevOps methodology and utilizing such as AWS CI/CD pipeline (CodePipeline, CodeBuild, and CodeDeploy).

1.4.5 IGA recommends going for Business Process Management (BPM) for business processes workflows for aligning business functions with customer needs.

1.4.6 iGA recommends going for open-source and cross-platform;

- Preferred: NodeJS/Java/.Net Core, etc.
- Least preferred: .NET as is it only working on various versions of Windows.

1.4.7 From its experience iGA advise to evaluate qualifying partners – like number and quality of AWS certified resources present locally/on ground to begin and operate the application.

1.4.8 Development of the Application must consider Scalability on the Cloud in order to maintain the concept of pay-as-you-go (preferred).

1.4.9 The ownership and Intellectual Property Rights (IPR) of the source code of the developed solution must be in the name of the entity. In case of a COTS product, the IPR of any customization done on the COTS product would be in the name of the entity.

1.4.10 IGA recommends using Source Code Management such as “Git.” Source code management as it enables coordination, sharing, and collaboration across an entire software development team.

1.4.11 The application software developed by the vendor has to be user friendly so that users can access it without having extensive training, therefore it is highly recommended that UI & UX are approved by the steering committee before the implementation phase.

1.4.12 The vendor must ensure the integration of the application with required monitoring platforms in iGA and NCSC for NOC and SOC operations. iGA has currently deployed "App Dynamics" as EMS tool, thus the vendor is required to consider the functionalities and features available in "App Dynamics" as EMS tool and design the monitoring of the application accordingly. The vendor is NOT required to provision for a separate EMS tool. However, the vendor would be required to coordinate with the entity for integration of the application with existing EMS so that requisite parameters may be configured in Dashboard, monitored and periodic reports may be generated.

1.4.13 The vendor shall provide interoperability support with regards to available APIs, data portability etc. for the entity to utilize in case of:

a. Change of Cloud Service Provider,

b. Migration back to in-house infrastructure,
c. Burst to a different cloud service provider for a short duration, or
d. Availing backup or DR services from a different service provider

1.6 Operations and Maintenance

1.6.1 iGA recommends that the operation and maintenance (O&M) phase would be for a period of 60 months from the Go-Live date with clear responsibilities defined for all stakeholders.

1.6.2 During the O&M phase, after Go-Live, the access / remote access to production environment (application and/or Database) will be made available from within the Kingdom of Bahrain. Further, it should be noted that remote access of production environment will NOT be made available to any resource of the vendor outside of Kingdom of Bahrain.

1.6.3 The entity must ensure that the vendor shall provide continuous support during phased roll out of the Application as well as during O&M phase and this must be in writing.

1.6.4 The entity must ensure that the vendor shall address all the issues/bugs/gaps in the functionalities of the application before the signed-off the SRS at no additional cost during the operations and management phase.

1.6.5 Incident management guidelines must be prepared by the vendors to define the proper approach to handle incidents during the O&M period on coordination with iGA.

1.6.6 Application monitoring will be the responsibility of the entity and iGA. The vendor is required to provide the requirements for application performance parameters in discussion with iGA, and count for the cost of AppDynamics licenses. The Infrastructure and Network monitoring feed would be provided to the vendor for "Dashboard view" for managing the SLAs by the entity and iGA.

1.6.7 The O&M scope should include clear activities for Knowledge Transfer and Handover and should be documented within the contract.

1.7 Deployment and Hosting

1.7.1 The implementation and hosting of the application would be governed by the iGA's Cloud First Policy released in April, 2017. It is expected that the vendor shall comply to the platform specification of AWS (iGA Latest Landing Zone).

1.7.2 All entity needs to seek iGA clearance for hosting the application on AWS Cloud, and make all changes mandated by iGA to meet the security requirements before the application is hosted at AWS cloud such source code review and vulnerability assessment.

1.7.3 DR configuration is required at infrastructure level in Active-Active or Active-Passive mode depending upon the solution requirements of the entity application. The entity might seek iGA alternative DR site whenever cloud is not appropriate alternative.

1.7.4 It is for information of the implementation team that the Application must be hosted within Shared Cloud such as Amazon Web Services (AWS) with hosting facility in Bahrain, that would be provided and managed by the entity with supervision from Information and eGovernment Authority (iGA).

1.7.5 The OS in all existing Cloud platform such as AWS and MS Azure is compatible with both Windows and Linux. However, Enterprise Linux is the preferred OS (such as SUSE). In case Windows OS is required, the currently supported versions are 2012 and 2012 R2, 2016 and 2019. The entity is not required to provision for licenses of OS on Cloud as it comes as managed services.

1.7.6 The existing standard Antivirus solution is Traps and can be supplied by iGA through NCSC.

1.7.7 The entity must ensure that the vendor is required to prepare and submit along with their technical proposal, the details of methodologies and computations for sizing and capacity of storage, compute, backup, network and security on the cloud.

1.7.8 There should be sufficient capacity (compute, network and storage capacity offered) available for near real time provisioning (as per the SLA requirement of the Contract) during any unanticipated spikes in the user load. The vendor will be responsible for adequately sizing the necessary compute, memory, and storage required, building the redundancy into the architecture (including storage) and load balancing to meet the service levels mentioned in the RFP.

Glossary

	Acronym	Description
1	**AWS**	Amazon Web Services
2	**BPM**	Business Process Management
3	**CI/CD**	Continuous integration/Continuous delivery
4	**COTS**	Commercial off-the-shelf
5	**DR**	Disaster Recovery
6	**EMS**	Environmental Management System
7	**iGA**	Information and eGovernment Authority
8	**NCSC**	National Cyber Security Centre
9	**NOC**	Network Operations Center
10	**O&M**	Operations & Maintenance
11	**OS**	Operating System
12	**PMO**	Project Management Office
13	**RDS**	Relational Database Service
14	**RFP**	Request for Proposal
15	**SLA**	Service-Level Agreement
16	**SOC**	Security Operations Center
17	**SRS**	Software Requirement Specification
18	**UI**	User Interface
19	**UX**	User Experience