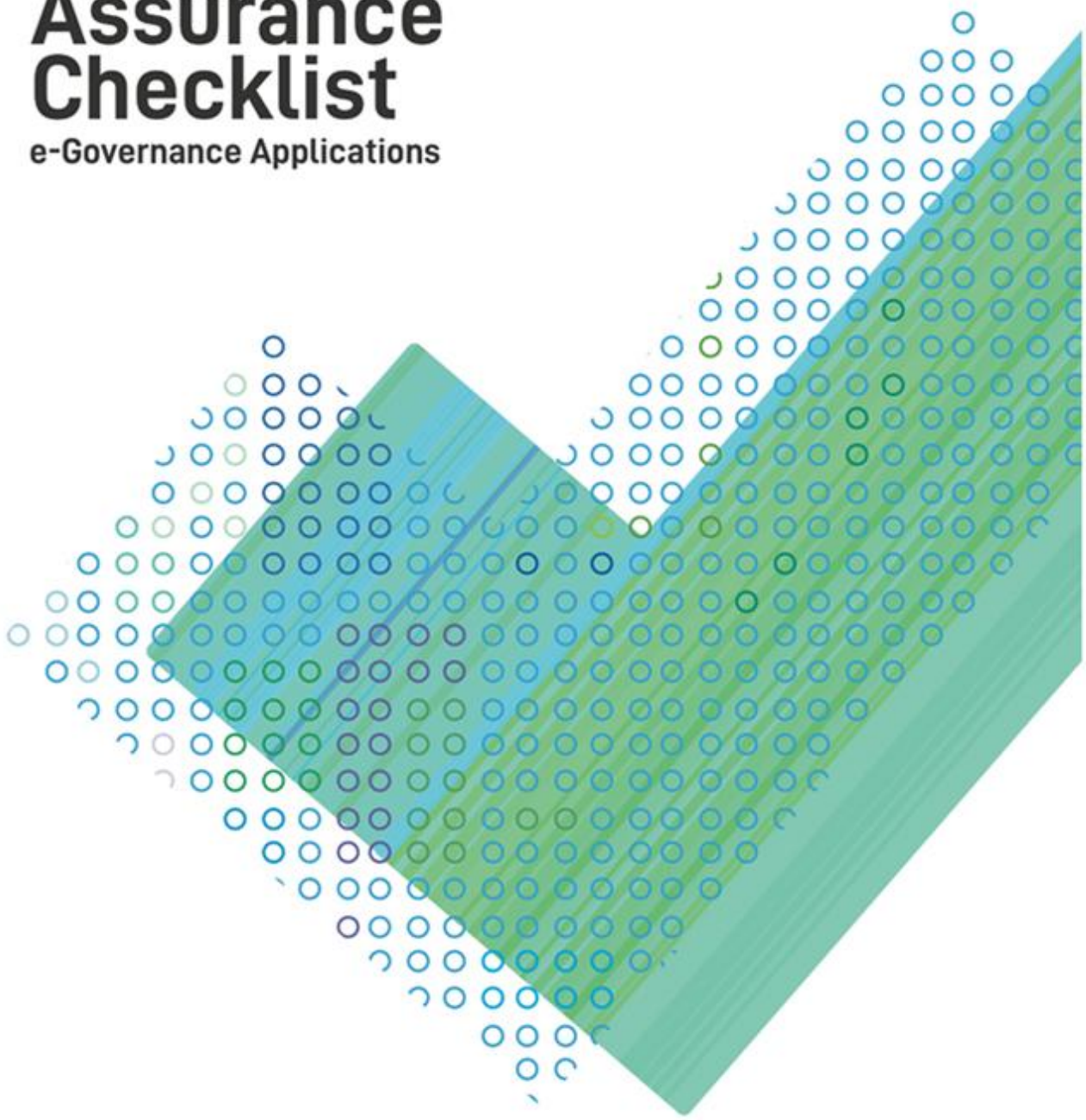
Quality Assurance Checklist

e-Governance Applications



NIC-SQG-CHK-001
(Version 1.1)
December 2018

NIC एनआईसी National Informatics Centre

Purpose

NIC is involved in design and development of large scale e-governance applications for various Ministries/Departments/State Governments. The quality of these applications in terms of functionality, reliability, performance, supportability, modularity, secuirty etc. is of paramount importance and can have impact on usability of these applications.

Based on the best practices, Software Quality Group has prepared basic quality assurance checklist for e-Governnance Applications.

The checklistlists out important basic quality attributes which needs to be incorporated in applications. These can be used as guiding principles while designing and development of e-Governance applications to meet basic quality requirements. This can also be used by project teams for self assessment of applications against these attributes.

The Software Quality Group will audit the applications against these features/attributes as it is expected that the applications devleoped by NIC meet these basic requirements.

Please forward your feedback/suggestions regarding this checklist to to Software Quality Group at **support-sqg@nic.in**

Project Details	
Ministry/State/Department	
Project Name	
HoD/Project Coordinator	

Sr. No.	Parameter	Conformance (Yes/No)
1.	***User Interface (UI)/User Experience (UX)***	
1.1	The **purpose**, **scope** and **intended audience** of Application is clearly specified on the **landing Page** of the application.	
1.2	Government of India,Ministry/Department and NIC **Logo(s)**are incorporated at appropriate place(s) at landing page. The header and footer of forms and reports also carries appropriate logos.	
1.3	The Users are able to clearly identify on the introductory/landing Page where to proceed for **Sign-Up/Sign In.** The **prerequisites** and **procedure** for **sign-up** has been clearliy specified.	
1.4	For Employee Centric and Ministry/Department Centric Application(s), **LDAP(**Lightweight Directory Access Protocol) **Authentication** is implemented. For LDAP Authenticaltion, the complete email address (like(abc.xyz@nic.in, abc.xyz@gov.in) is used as Login ID.	
1.5	'**Forgot Password**' and '**Change Password**' processes are implemented. The ***Password quality*** is implemented as per NIC Password Policy. (Refer http://security.nic.in for NIC Password Policy)	
1.6	**Proper Authentication** mechanism(single factor authentication, two-factor authentication or multi-factor authentication) has been implemented as per sensitivity of the application.	
1.7	The **Sensitive Personal Data or Information** (SPDI) like Passwords,Financial Information(e.g. bank account, credit card details etc.),Biometric Information(e.g. Adhaar No., Driving Licence No. etc). is **not displayed/published** publically.If required, it is **masked** on display.	
1.8	The application is well **responsive to any device**(desktop, laptop, tablet, mobile) i.e. the application user interface flawlessly align depending on the resolution and dimensions of the device. (Responsive Design Mode feature available in browsers like Mozilla Firefox/ Google Chrome can be used to validate if the Application supports/fits different devices.)	
1.9	**No feature** of the application is **Browser dependent**. It functions properly across latest versions of the popular browsers(Internet Explorer, Mozilla Firefox, Chrome, Safari, Edge).	
1.10	All **exceptions/errors** are displayed as **user interpretable** (User Friendly messages) and not as system default errors. The application implements required validations to **protect users against making mistakes.**	
1.11	The application provides necessary tools like User manual, Help, FAQs etc. to enable the **user to learn to use the product** with **effectiveness** and **efficiency.**	
1.12	The labels, menu options, drop down lists, radio buttons, Inline Text, directories etc. and other related **content** in the application has been checked for any **spelling / grammatical errors**.	
2.	***Forms and Reports***	
2.1	**Required(**Mandatory) and **optional** fields are clearly marked. **Required fields** are indicated by a **asterisk (*).**	
2.2	**Primary Action Buttons** (Save,Submit or Continue) are kept **prominent** in form. If **Secondary ActionButtons** (Cancel, Reset or Back) are incorporated **less visual weight** is given to them.	
2.3	**Field level validations** and **Form level validations** are carried out at appropriate events. Appropriate messages are displayed for validation and exceptions handling. **The client side** and **server side** validations are incorporated in the application.	
2.4	The **large web forms** are divided into **logical data collection** parts. They are split into multi-step filling up option (like using Tab forms). The **objective** of the form and any **external information** (Like AAdhar Number, PAN Card, scan documents etc) requirment necessary for completion of the form are clearly mentioned to the user as part of **Form filling instructions**.	
2.5	For large web forms, **Auto Saving feature** is implemented so that there is no loss of data and user is able to continue from the point left.	
2.6	Before performing **Update, Delete and Cancel** operation, a **confirmation message** is displayed.	
2.7	The **restrictions**(File Type, size etc.) related to **document/image upload** is clearly indicated and incorporated.	

2.8	The application provides option to the user to **export report** output to **PDF/Excel or any other format** as per requirement.	
2.9	The application implements **proper secure permissions**such that acess to report data is Role Basedand provide option to the Admins for **permission management**.	
3.	***Data Quality, Management and Security***	
3.1	Domain specific **Master code directories** are identified and codified. The **location directory** (State, Distrcit, Village, Panchayat etc are adopted from LG Directory(http://lgdirectory.gov.in) and Controlled Vocabulary Services (http://vocab.nic.in)). Proper mechanism is incorporated to ensure that **master code directories** are in **sync** with the the **source** (using Web Service or maintaining a local copy)	
3.2	**Database schema** is designed with **domain specific attributes** and **normalised** to a required level. All **key attributes** and **constraints**are defined.	
3.4	The application has built in mechanisms and **tools** to reduce or eliminate the need for **direct access/updation at Database** level.	
3.5	**Role based access control (RBAC)** functionality enables application administrators to limit and **control the permissions** of users. At the most basic level, the roles : Super Admins, Admins, Users, Reporting Users and Read only users are considered for the application. The application implements the **principle of least privilege**.	
4.	***Technology, Frameworks and Deployment Architecture***	
4.1	The application is built **on latest stable versions of technologies/frameworks**.	
4.2	The **deployment architecture** is worked out by estimating critical parameters like number of hits, total number of users, concurrency, number of transactions, peak load, high availability requirements etc.. The Architecture is **horizontally scalable** and ensures that there **is no single point of failure** for critical applications. *(Refer "Building Scalable Web Applications" document at Digital NIC : Knowledge Café ->Software Quality Tab.)*	
4.3	The minimum **Response Time** for any page loading or action performed in the application is within 5sec, exceeding which, appropriate message is displayed.	
5.	***Log Management***	
5.1	**Audit logging feature** is built to log relevant activity into a system that is **time synced** and **accessible to the applicationadministrators** through UI.	
5.2	All important events in application (like successful and failed login attempts) and on data are recorded. When an **event is logged** it should have details that provide enough information about the event to provide the necessary context of **who, what, when and where**. The critical fields like Username/User ID, IP Address of Terminal, Server time, object which is changed,Action which changed the object, Action Type (C R U D) and brief description of the Action are recorded.	