|  |  |  |  |
| --- | --- | --- | --- |
| **Review Reference No.:** |  | **Review Date:** |  |
| **Review Reference Documents:** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Sl No.** | **Description** | **Yes/No/NA** | **Actions To Be Taken/ Remarks** |
| **Clarity** | | | |
|  | Are the characteristics of users and of typical usage mentioned? (No user categories missing.) |  |  |
|  | Does each requirement have a unique identifier |  |  |
|  | Do the requirements express actual customer needs (in the language of the problem domain), rather than solutions (in developer jargon)?  (check if the requirements are written in non-technical, understandable language) |  |  |
|  | Is there a Glossary in which the specific meaning of each term (Domain Dictionary) presents? |  |  |
|  | Is each requirement atomic and simply formulated? (Typically a single sentence. Composite requirements must be split.) |  |  |
|  | Are Requirements organized into coherent groups? |  |  |
|  | Are all unstable requirements marked as such (TBC= To be confirmed, TBD = To be defined) |  |  |
|  | Are there any requirement which could have more than one interpretation? |  |  |
| **Prioritization** | | | |
|  | Is each requirement prioritized? (is the meaning of priority levels clear) |  |  |
| **Completeness** | | | |
|  | Does the Requirement Specification document address the following sections at a minimum under ‘General’ Category   * Introduction * Scope * Definitions, Acronyms and Abbreviations * Constraints * Assumptions & Dependencies (relating to Business, Functionality, Hardware, Software) * Necessary Appendixes, Diagrams/Tables |  |  |
|  | Are all of the requirements related to the following defined:   * Business * Functionality based * Non –Functional Requirements (Performance, Usability, Reliability, Security, Maintainability) * Hardware /Software (For projects involving both software and hardware, are system requirements clearly defined and documented?) * Database * External /Internal interfaces * Input/Output * Reporting |  |  |
| **Change Management** | | | |
|  | Is the change management process of requirements clearly defined and understood? |  |  |
|  | Are possible changes to requirement specified? |  |  |
|  | Is the likelihood of change specified for each requirement? |  |  |
|  | Is the requirement document clearly and logically organized so as to support modifiability/change at any point of time? |  |  |
| **Traceability** | | | |
|  | Are all the requirements traceable back to a specific user need?  Are all requirements traceable forward to a specific software module?  Is there a supporting table mapping each business requirement to Functional requirements/modules?)  Are all requirements traceable forward to a specific design document? |  |  |
|  | For integrated projects - Has traceability of system level requirements (overall program) to subsystem level requirements (individual projects) been established? |  |  |
| **Consistency** | | | |
|  | Are there any requirements describing the same object that conflict with other requirements with respect to terminology? |  |  |
|  | Are there any requirements describing the same object that conflict with respect to characteristics? |  |  |
|  | Are there any requirements that describe two or more actions that conflict logically? |  |  |
| **Verifiability** | | | |
|  | Are all the requirements feasible and testable (in a provisional acceptance test) |  |  |
|  | Are there any requirements which will be expressed in verifiable terms at a later time? |  |  |
|  | Have all the affected groups reviewed the requirements? |  |  |
|  | Are commitments from affected groups to meet the requirements mutually agreed upon? |  |  |
| **Validation** | | | |
|  | Are the acceptance and performance criteria defined for the requirements?  (Has the target environment been identified and documented)  Are all external dependencies, which might affect acceptance test such as test data availability, tools etc., documented?  Are the duration, effort and locations for Acceptance Testing agreed upon?  Is the review and approval authority clearly identified for RS and Acceptance Test?  Are issues affecting validation of the product identified and resolved? |  |  |
| **Security - General** | | | |
| 26. | Has the nature of the the system- Client-Server/ Intranet / Internet/ Extranet based been captured? |  |  |
| 27. | Have the 3rd Party Software to be used by the system captured along with purpose of usage? |  |  |
| 28. | Has the open source software to be used by the system captured along with the purpose of usage? |  |  |
| 29. | Has the technologies/ framework to be used for developing the application been identified? (For e.g. J2EE, .NET, Struts, Spring, Hibernate etc.) |  |  |
| 30. | Are compliance objectives been identified? |  |  |
| 31. | Are levels of confidentiality defined? |  |  |
| 32. | Are levels of integrity guarantee captured? |  |  |
| 33. | Are the system availability guarantees captured? |  |  |
| 34. | The access control to be utilized by the system – is it defined? |  |  |
| 35. | Are the measures the system utilize to protect against insider threats defined? |  |  |
| 36. | Is the type of intrusion-detection measures that should be in place captured? |  |  |
| 37. | How should the system record intrusions and intrusion responses, if at all? |  |  |
| **Security – Authentication** | | | |
| 38. | Does the systems use one of the following techniques for authentication?   * User ID & Password /PIN * Digital Certificates * Biometric |  |  |
| 39. | Does each user login with a unique user ID? |  |  |
| 40. | Are the application users different from database users? |  |  |
| 41. | Does the system impose a restriction on the length and structure of the password to make it difficult to guess? |  |  |
| 42. | Is the system responsible for storing password? If yes, then is the password one way hashed? |  |  |
| 43. | Does the system ensure that passwords are changed frequently by setting the password expiry period? |  |  |
| 44. | Is the mechanism how the login credentials are passed from browser/ client to server captured? |  |  |
| 45. | Does the system ensure to encrypt the login credentials over the network? If yes, which algorithm will be used for this purpose? |  |  |
| 46. | Does the system limit each user ID to one simultaneous logon session? |  |  |
| 47. | Does the system lock user account after a designated number of consecutive unsuccessful attempts? |  |  |
| 48. | Does the system log activities involving authentication credentials?  (This includes successful login, unsuccessful & failed attempts and reset logins) |  |  |
| 49. | Does the system prohibit authentication credentials from being captured in log files? |  |  |
| **Security - Authorization** | | | |
| 50. | Does the system propose a mechanism for authorizing users? (E.g. Access Control Lists, Access Matrix, Role Based, Rule-Based, etc.) |  |  |
| 51. | Does the authorization mechanism ensure that users are only allowed to do what they permitted to do? |  |  |
| 52. | Does the system prevent direct access of database? |  |  |
| **Security – Data Validation** | | | |
| 53. | Does the system define a mechanism to validate the input data before being processed by any application component? |  |  |
| 54. | If the system has interfacing with external sources, then is the emanating data validated before being processed? |  |  |
| 55. | Is it intended to have reusable components / generic libraries for implementing data validation? |  |  |
| **Security – Session Management** | | | |
| 56. | Does the system define session tracking mechanism (Cookies or Embedded Session data)? |  |  |
| 57. | Does the system define maximum session lifetime? |  |  |
| 58. | Does the system maximum renewable session timeout? |  |  |
| 59. | Does the system prompt the user to login to the application again, after a session is expired? |  |  |
| **Security - Cryptography** | | | |
| 60. | Does the system define encryption mechanism for sensitive data wherever required? |  |  |
| 61. | Is the encryption algorithm identified? |  |  |
| 62. | If Digital Certifications are intended to be used for authentication, then has the system identified a policy for key management? (i.e. generation/ protection/ expiration/ information recovery of Private Key) |  |  |
| **Security - Error / Exception Handling** | | | |
| 63. | Does the system define error handling mechanism to recover gracefully from anticipated user errors (e.g., invalid input)? |  |  |
| 64. | Does the system plan to handle unknown error messages/conditions to avoid information leakage? |  |  |
| 65. | Does the system define error handling mechanism to recover gracefully from anticipated user errors (e.g., invalid input)? |  |  |
| **Security - Logging** | | | |
| 66. | Has the system identified the requirement of logging the activities? |  |  |
| 67. | Has the system identified to log the user name, time of operation for each of the operations (Insert, Update and Delete)? |  |  |