| 40  step | Data flow delivery checklist | | Data flow name and version |  | | | *This checklist must be completed and approved before deployment in OMNIA* | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Developer(s) |  | | |
|  | | | | | | | | | | |
|  | | *Data flow solution requirement/capability to be reviewed and approved* | | | *Status* | *Comment* | | *Approval* |  | *Guidelines* |
| **Design review**  done by a peer before starting development of new solution or major changes | | 1. Data flow name. When available, application name should be part of the name. | | |  |  | | Review  done by: <short name(s)>  Approved:  <date> |  | Enter relevant cell shading color (no text) in each Status column cell after the review: |
| 1. Solution design and technology used | | |  |  | |  |
| 1. Access and secret management solution | | |  |  | |  |
| 1. Security risk of IT components approved | | |  |  | |  |
| 1. Legal risk of data transfer to OMNIA approved by data owner | | |  |  | |  |
| 1. Data democratization: Data available in DLS, and for data analysts and data scientists | | |  |  | |  |
| **Development review**  done by a peer developer before deployment to test environment | | 1. No basic flaws or problems | | |  |  | | Review  done by:  <short name(s)>  Approved:  <date> |  |
| 1. Component naming according to standard | | |  |  | |  | Green = OK |
| 1. Shared OMNIA components used when appropriate | | |  |  | |  |  |
| 1. All functions documented in source code | | |  |  | |  | Orange = should be corrected,  but will be accepted |
| 1. No passwords nor service principal keys in code | | |  |  | |  |
| 1. No dead code (limit cruft, no dead code without justifying comment) | | |  |  | |  |
| 1. Project is split reasonably (ref. [Curly’s law: Do one thing](https://blog.codinghorror.com/curlys-law-do-one-thing)) | | |  |  | |  |
| 1. Configuration strings externalized into (a) configuration file(s) | | |  |  | |  |
| 1. Application settings and variables specified in system configuration section in runbook | | |  |  | |  |
| 1. No passwords nor service principal keys in config files | | |  |  | |  |  |
| 1. All artifacts (e.g. scripts for stored procedures and table definitions) in GitHub | | |  |  | |  | Red = must be corrected to pass approval |
| 1. Repository structure in GitHub, incl. correct release/version number in GitHub | | |  |  | |  |
| 1. Runbook | | |  |  | |  |
| 1. Developer(s) named in runbook | | |  |  | |  |
| 1. External dependencies documented in runbook | | |  |  | |  | If status is orange or red, a brief explanation should be provided in the Comment column cell.  Extended explanation can be included below the checklist table (referring to the checklist item number). |
| 1. readme.md on GitHub, including installation instructions | | |  |  | |  |
| 1. System diagram updated to reflect solution | | |  |  | |  |
| 1. All components included in deployment scripts | | |  |  | |  |
| 1. Any deployment work outside running the scripts is documented | | |  |  | |  |
| 1. Proper testing done in development environment | | |  |  | |  |
| 1. Test cases passed | | |  |  | |  |
| **Production review**  done by a peer developer before deployment to production environment | | 1. Solution running ok in test environment | | |  |  | | Review  done by:  <short name(s)>  Approved:  <date> |  |
| 1. Documentation updated with enough details | | |  |  | |  |
| 1. Data flow diagram included in runbook | | |  |  | |  |
| 1. Exceptional error situations documented in runbook | | |  |  | |  |
| 1. Contact information for customers available in runbook | | |  |  | |  |
| 1. Data catalog updated | | |  |  | |  |
| 1. Data deleted in development and test environments | | |  |  | |  |
| 1. Data flows deleted or paused in development and test environments | | |  |  | |  |
| 1. Deployment instructions/description (script) incl. steps, data flow name etc. | | |  |  | |  |
| 1. Data flow components secured with the minimum requirements | | |  |  | |  |
| 1. Relevant user names/passwords/keys stored in a Key Vault | | |  |  | |  |
| 1. Passwords meet complexity requirements | | |  |  | |  |
| 1. Web application secured against common threats | | |  |  | |  |

Other information considered important for the approval of this checklist can be included below. This document should be stored along with other solution documentation in the ODET2 library.