Business

Applications-Information Security Process

|  |  |
| --- | --- |
| ***DOCUMENT RELEASE NOTICE*** | |
| **Information Security process – New applications**  Release No 0.1 | |
| Author(s): GayathriKandasamy | Date: 10th June 2017 |
| Reviewer(s): Radhakrishna | Date: |
| Approved by: | Date: |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Revision History*** | | | | |
| *Release No.* | *Release Date* | *Change Details* | *Prepared/*  *Amended By* | *Reviewed By* |
| 0.1 | 10th June Aug 2017 | Draft | GayathriKandasamy | Radhakrishna |
|  |  |  |  |  |

**Table of Contents**

[*1* *Objective* 4](#_Toc486590200)

[*2* *Target audience* 4](#_Toc486590201)

[*3* *Roles and responsibilities of stake holders* 4](#_Toc486590202)

[*4*  *Security review process* 5](#_Toc486590203)

[*5* *Information & Initial update requirements* 6](#_Toc486590204)

[*5.1* *A Brief description of the business solution* 6](#_Toc486590205)

[*6* *Security requirements in details* 7](#_Toc486590206)

[*I.* *Data flow diagram* 7](#_Toc486590207)

[*II.* *External Connection requirements (If applicable)* 7](#_Toc486590208)

[*III.* *Interface Descriptions* 7](#_Toc486590209)

[*IV.* *Process related controls* 8](#_Toc486590210)

[*V.* *Vulnerability Management Controls* 9](#_Toc486590211)

[*VI.* *IT Infrastructure setup* 9](#_Toc486590212)

[*VII.* *Vaulting requirements* 10](#_Toc486590213)

1. ***Objective***

*The purpose of this document* is to establish guidance and information on control framework for Business applications structured security review and to provide step by step process for Information Risk Assessment process for new application deployment. Document also provides list of information requirements to help IT Security team to assess and fasten the Risk Assessment process.

1. ***Target audience***

* Application Asset Owner
* IT team, application development
* IT Security team
* IT Infrastructure team
* Application Support

1. ***Roles and responsibilities of stake holders***

Roles & Responsibilities for completing security review and Application Risk Assessment process is summarized below

|  |  |
| --- | --- |
| Title | RACI matrix |
| Application(Asset) owner | * Assigns data classification levels for the application * Ensures implementation of key control requirements * Reviews & sign off on deviation requirements if any * Ensures that the access to the system is provided on need to have basis through authorization process and periodic reviews |
| Development team ( Internal or vendor) | Provide application specific control information. Ensures effective implementation of IT Security controls |
| India IT – IT infrastructure | Providers implementation support  Ensures that the IT infrastructure used for hosting application is configured secured |
| IT Security | Provides guidelines on IT Security requirements  Reviews effectiveness of IT Security controls implemented  Issue final Risk Assessment report |
|  |  |

***4 Security review process***

Security review of process will follow following standard process for risk identification, mitigation and action planning.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sl No** | **Key activity** | **Deliverables** | **Activities** | **Responsibility** |
| Step 1 | Business Impact Assessment ( BIA) | To identify data classification level, RTO, RPO values for the planned implementation | 1.To identify Business owner & Application custodian for the application  2. To update IT Security on the planned activity with application & Business process brief  3. To issue BCQ ( Business criticality questionnaire)  5. to complete BIA process | 1,2,. Business  3- IT Security  4- Business |
| 2 | Information Security Questionnaire (ISQ) | To assess ISP compliance statusof new applications | 1. Control requirements through a set of questionnaire sent to the Application custodian  2. Application custodian to be update the status informationand complete the ISQ process | Application Custodian |
| 3. | Technical Details Questionnaire (TDQ) | To get know the functionality and the technical details about the application | 1. 1.It is a continuation of ISQ and issue the Technical Details Questionnaire  2. the application custodian will update technical details of the application  3. To define required processes & Procedures  4. Complete the TDQ process  5. Security penetration testing/source code review | 1 – Security  2,3,4 –Application custodian |
| 4. | External Vendor Questionnaire(***only for applications hosted with Third Party***) | To assess and record the security capability of a Third Party Supplier. | 1. This assessment will cover the key security control areas as part of the assessment process control implementation from vendor site.  2. The External Vendor Questionnaires will be circuited to the Third party supplier.  3. Complete the EVQ process | 1,2, – Security  4 – Third party supplier/ Application custodian |
| 5 | Information Risk Assessment Report | To assess and issue Final IRAP Report | IT Security to assess status of control implementation in line with ISP requirements and issue final Risk Assessment report (*IRAP).* | IT Security |
| 6 | **IRAP report closure** | IRAP report closure | 1.Business to update and finalize the action plan for the IRAP finding  2.To update deviations & Risk Acceptance if any | 1. Application Owner & IT Security |

***5 Information & Initial update requirements***

## *5.1 A Brief description of the business solution*

*<Business team to provide a brief overview of the proposed system /application and business processes related to >*

*5.2 Application & other related information*

Please provide the details as requested below.

|  |  |  |
| --- | --- | --- |
| **Sl.no** | **Information requested** | **Updates /Remarks** |
|  | Application Name& Version | TaxBreeze |
|  | Application owner ( with GUID) |  |
|  | Project Name /Project Code |  |
|  | Application custodian ( with GUID) |  |
|  | Developer/Manufacturer |  |
|  | Vendor Name , If Involved |  |
|  | Engagement Partner Name |  |
|  | Is the application web based/Mobile App Based or both | Web Based |
|  | Is the application Internal /Internet facing application | Internet |
|  | Hosting information( Like in Azure cloud, PwC India Data center) | Azure Cloud |
|  | If the application is not hosted in Azure or PwC India data center, has the third party hosting provider certified for ISO 27001/SOC2? | No, It is hosted in Azure |
|  | Application and/or database Managed, supported by PwC India or Vendor. If managed by third party pls provide vendor details and location from which the support will be provided | PwC India |
|  | Approximate no. of internal /external users | 20/10000+ |
|  | Does the application provide payment processing facility | Yes |
|  | Database & OS & Web server version details | SQL DB, Windows | |
|  | Status of Application penetration testing ( If completed, please attach latest report) | NA | |
|  | Status of Security Code Review report of the application. Please attach latest review report if completed |  | |
|  | Details about the data Encryption Mechanism in place. To confirm if the data is encrypted in store and in transit | DEA to help | |
|  | Is the user on boarding /off boarding process in place? If yes, pls attach related document | Kayur to help | |
|  | Does the application support 2 factor authentication mechanism | No, But will implement in phase 2 | |
|  | Pls update on the application DR requirements | DEA to provide | |
|  | Details of the backup /retention requirements | Enable back up in azure | |
|  | Pls update on availability of separate development and test environment | Yes | |
|  | Does the application store /process Personally Identifiable Information ( PII) | Yes | |

***6 Security requirements in details***

## *Data flow diagram*

<Copy & Paste the relevant diagrams detailing application, interface with other system and proposed network architecture>

Not Applicable for the tool

## *External Connection requirements (If applicable)*

Not Applicable for the tool

## *Interface Descriptions*

Not Applicable for the tool

|  |  |
| --- | --- |
| **Parameters** | **Description** |
| Interface Name |  |
| Interface business Objective | <Description of interface objectives, why it’s used, what data etc.,> |
| Interface Type | STP  Batch Interface |
| Interface Method | Batch  online  Manual SFTP |
| Interface Direction | Both inbound and outbound |
| Details of data/message flow | Both inbound and outbound |
| How data integrity is ensured |  |
| Frequency of file transfer | Daily basis |
| File naming convention |  |
| Source folder with IP address |  |
| Destination folder with IP |  |
| Acknowledgement expected |  |
| **Comments :-**< Insert comments on control implementation (if any) > | |

|  |  |  |
| --- | --- | --- |
| **Data Protection Controls** | | |
| Control Area | Control Description | Compliance(Yes/No)  with details/comments |
| Data privacy | Data sanitization should be performed before moving the production data to Test and Development environment. Scripts should be made available for data masking. | No |
| Segregation of Environment | Segregation among Production, Test and Development environment should be ensured. Test environment should be running with the same version of application and all other underlying components | Yes |
| < Insert description of control implementation > | | |

## *Process related controls*

(To be implemented by Asset Owner)

* 1. *Authorization Matrix- Sample*

**Key**

* V: Only View
* AED: Add/Edit/Delete functions
* R: Review
* A: Add function

**Roles:**

* PwC User: **PU**
* P&G User: **PG**
* Distributors: **D**

**Tasks**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S.No** | **Task** | **PU** | **PG** | **D** |
| **1.** | **Add Distributor** | *AED* | *V* |  |
| **2.** | **Add Branches** | *AED* | *V* | *V* |
| **3.** | **Create forms for specific states** | *AED* |  | *V* |
| **4.** | **Information in the forms** | *R* |  | *AED* |
| **5.** | **Sample documents** | *AED* |  | *V* |
| **6.** | **Comments on Documents received** | *A* |  | *V* |
| **7.** | **Dashboard** | *A* | *V* | *V* |
| **8.** | **Status of Application** | *A* | *V* | *V* |

* 1. *BCP plan*

*Detailed Business Continuity Plan is required to be defined along with testing frequency in consultations with IT security team*

* 1. *DR plan*

*DR plans along with DR run books needs to be defined and documented, in case of DR requirements, procedures to be provided by IT. DR plans to include data backup & Restore plans*

## *Vulnerability Management Controls*

*(To be coordinated by IT and signed off by IT Security)*

|  |  |  |
| --- | --- | --- |
| **Technical Vulnerability Management Controls** | | |
| Control Area | Control Description | Compliance(Yes/No)  with details/comments |
| Secure Code Review / Dynamic Scanning | Code Review has been performed before moving into production ( for external facing applications, scope to be decided in consultation with IT Security) |  |
| Penetration Testing | Penetration has been performed before moving into production.( scope to be decided in consultation with IT Security | NA |
| Vulnerability Assessment | VA is performed on all the components before moving into production. Also an annual audit is performed to ensure continued compliance | NA |
| Patch mgmt | Application and all other components are part of patch management calendar | NA |
| Anti-virus Control | Anti-virus software is running in all components and virus definitions are getting updated centrally | NA |
| **Comments :-**< Insert comments on control implementation (if any) > | | |

## *IT Infrastructure setup*

|  |  |  |
| --- | --- | --- |
| **IT Infrastructure Controls** | | |
| Control Area | Control Description | Compliance(Yes/No)  with details/comments |
| Baseline security controls | Base line security controls as suggested as best practices to be implemented at OS level |  |
| Baseline security controls | Base line security controls as suggested as best practices to be implemented at OS level |  |
| Password vaulting | privileged accounts and service account information to be kept in a secure vault |  |
| **Comments** :- < Insert comments on control implementation (if any) > | |  |

## *Vaulting requirements*

(To be done where applicable)

|  |  |  |
| --- | --- | --- |
| **Key Management Controls** | | |
| Control Area | Control Description | Compliance(Yes/No)  with details/comments |
| Key Inventory | Inventory of all cryptography keys, smart cards, dig. Certificates should be maintained along with details of ownership and expiry details |  |
| Safe custody | Cryptographic keys associated with the application should be kept under safe custody |  |
| Password vaulting | Application privileged accounts and service account information to be kept in a secure vault |  |
| **Comments** :- < Insert comments on control implementation (if any) > | |  |