**This form will be filled up by Application Owner or System Owner or Business User when not able to implement IT Security Requirements within the expected timeline.**

|  |
| --- |
| 1. **Requester Information:**
 |
| Requester Name: | AZYAN BINTI AYUB |
| Job Role: | CDB PENTEST SPA YEAR 3 |
| Email: | azyan@bsn.com.my |
| Phone: | 0176935009 |
| Dept or Div.:Request Date : | JTM/AM – DIGITAL BANKING13/07/2023 |
| 1. **Exception for:**
 |
| **System Name: CDB** |  |
| *Please tick system is deviating from which IT Security Requirements* |
| [ ]  System Hardening[ ]  IT Security Checklist | [x]  IT Security Assessment[ ] Access Management Guidelines | [ ] Patch Management Process[ ]  IT Security Checklist[ ] Others \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. **Justification/Reason for Exception** *(Details as per Appendix 1 or 2):*
 |
| The remediation was put on hold due to priority given to DuitNow and QR project which should be complete by Q4There are total 1032 High findings, 6574 Medium findings, 1142 Low findings and 6 info to remediate for CDB which include Int PT, HA Config, DB Config, WAPT, MAPT and Ext PT. The remediation will be done by phase as per below target date:1. Batch 1: 31st Aug 2023
2. Batch 2: 31st Dec 2023

Please refer Appendix for details finding:1. 2022 BSN CDB Database Configuration Assessment Quick Results-v1.0
2. 2022 BSN CDB eBiz Mobile Application Penetration Test (White Box) Quick Results-v1.1
3. 2022 BSN CDB External Servers Penetration Test (Black Box) Quick Results
4. 2022 BSN CDB Front End Portal Web Application Penetration Test (White Box) Quick Results-v1.0
5. 2022 BSN CDB Host Configuration Assessment Quick Results-v1.0
6. 2022 BSN CDB Internal Servers Penetration Test (White Box) Quick Results-v1.0
 |
| 1. **Options and cost to comply:**
 |
| The cost of enhancement will be identify after assessment completed. |
| 1. **Overall Residual Risk:**

*Please refer to Appendix 3 for RISK IMPACT & LIKELIHOOD from the RMF* | [ ]  **High** [ ]  **Medium** [ ]  **Low** |

|  |
| --- |
| 1. **Requestor**
 |
| **Prepared By** *(Application/System)* **:** | **Reviewed By** (HOS *Application/System) :* |
|  |  |
| Name: AZYAN BINTI AYUB Date: 13/07/2023 | Name: YUSREE NASIR Date: 13/07/2023 |

|  |
| --- |
| 1. **Reviewer**
 |
| **Reviewed By** (Manager, *Application/System) :* | **Reviewed By** (Manager, IT Security*) :* |
|  |  |
| Name: HELNIZA CHEK ANY Date: 13/07/2023 | Name: MOHD AIDIL MOHD RAHIM Date: |

|  |
| --- |
| 1. **Approver**
 |
| **Risk Accepted By** *(HOD of Business Owner / Deputy of HOD for ITD-related system):* | **Approved / Rejected By**  *(HOD of ITD):* |
| *This exception is:* [ ]  Approved [ ]  Rejected  | *This exception is:* [ ]  Approved [ ]  Rejected  |
| Name: Date: | Name: Date: |

|  |
| --- |
| 1. **ITRWC (IT Operation) /PSC (Project) Approval** *(if the request was rejected by HOD of IT)*
 |
| [ ]  Approved [ ]  Rejected **Date of ITRWC/PSC meeting:** *(To attached presentation slides and signed-off MOM)* | Approval / rejected remarks: |
| 1. **Administration** *(To be completed by SPP, IT Security):*
 |
| **Reference No :** | **Reviewed by:**Name: Date: |
| **Remarks :** |

**Appendix 1**

**List of Exception Items**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **No.** | Name of System / Application | **Non-Compliance Items / Clause** | **Residual Risk** | **Compensating Control** | **Action Plan for Closure & Target Date** | **References / Remarks** |
| Impact | Likelihood | Overall |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

*Please add row if more than 10 exceptions. You may attached the supporting documents for approver’s references.*

**Appendix 2**

**List of Exception for Pentest Remediations**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No** | **Vulnerability Category** | **Vulnerability Name** | **Effected Host** | **Effected segment** | **Access Level** | **No of Related Findings** | **Recommended Solution** | **Compensating Control** | **Action Plan (Provide Timeline/Target Date)** |
|  |  |  |  |  |  |  |  |  |   |
|  |  |  |  |  |  |  |  |  |   |
|  |  |  |  |  |  |  |  |  |   |
|  |  |  |  |  |  |  |  |  |   |
|  |  |  |  |  |  |  |  |  |   |
|  |  |  |  |  |  |  |  |  |   |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

*Please add row if more than 10 exceptions. You may attached the supporting documents for approver’s references.*

***Appendix 3***

*List of Risk Impact & Likelihood (Reference from Risk Management Framework – RCSA Checklist*







