

DTI PMO Template 403

Security Assessment Report

Project name & ID

Document Author: Insert name

Date Created: Insert date

Template Data

|  |  |  |  |
| --- | --- | --- | --- |
| Title | DTIPMO403 Security Assessment Report | | |
| Description |  | | |
| Template ID | DTIPMO403 | Classification | Internal Use Only |
| Template Owner | DTI PMO | Template Approver | Head of DTI |

## 

Template Revision History

|  |  |  |
| --- | --- | --- |
| Date | Author | Revision |
| 15th October | DTI PMO | Draft Template Rebrand & Naming convention |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**executive summary**

Background

Provide brief background of the project, the assessment scope and objective.

Risks

The summary of risks identified during the Security Assessment exercise is outlined here.

* **Risk 1 –** Description (1 line).
* **Risk 2 –** Description (1 line).
* **Risk 3 –** Description (1 line).
* **Risk 4 –** Description (1 line).
* **Risk 5 –** Description (1 line).
* **Risk 6 –** Description (1 line).
* **Risk 7 –** Description (1 line).
* **Risk 8 –** Description (1 line).
* **Risk 9 –** Description (1 line).
* **Risk 10 –** Description (1 line).
* **Risk 11 –** Description (1 line).

It also includes an overall risk profile of the application based on its exposure to sensitive information it stores, process or handles and the subsequent impact the identified security risks has on Etihad operations, business, reputation and legal requirements of the Organization.

**Detailed Risks and agreed actions**

| **RISK DETAILS** | **ACTION PLAN / RECOMMENDATION** | **ACTION PLAN OWNER** | **STATUS REMARKS** | **TARGET CLOSURE DATE** | **RATING** |
| --- | --- | --- | --- | --- | --- |
| ***Risk Title (Category – Very High, High, Medium, Low, Very Low):***  xxxxx.  ***Potential Consequences:***  xxxxxx. | * xxxx. | <Name & Title>. |  |  |  |

**Recommendation**

<Provide appropriate recommendation in relation with whether Information Security recommends the application to Go Live based on the status of identified risks if adequately addressed.>.

**Appendix 1 – Risk Rating Criteria**

|  |  |  |
| --- | --- | --- |
|  | Very high | * It will have major effect on security posture and brand value of the organization * Affects majority of all critical services or entire operations of EAG * All or most of sensitive information stored or processed can be compromised * Exploitation significantly increases the probability of additional vulnerabilities being exploited * Major non-compliance with mandatory requirements of organization’s policies and legal, regulatory & statutory regulations and standards. |
|  | High | * It will have substantial effect on security posture and brand value of the organization * Affects considerable amount of critical services and operations of EAG * Considerable % of sensitive information stored or processed is compromised * Exploitation increases the probability of additional vulnerabilities being exploited * Considerable non-compliance with some of the mandatory requirements of organization’s policies and legal, regulatory & statutory regulations and standards. |
|  | Medium | * It will have limited effect on security posture and brand value of the organization * Affects limited amount of services and operations of EAG * Limited % of sensitive information stored or processed is compromised * Exploitation could increase the probability of additional vulnerabilities being exploited * Partial non-compliance with some of the mandatory requirements of organization’s policies and legal, regulatory & statutory regulations and standards. |
|  | Low | * It will have a minor effect on security posture and/or brand value of the organization * Affects insignificant amount of critical services and operations of EAG * Insignificant % of sensitive information stored or processed is compromised * Effect of vulnerability is tightly contained, does not increase the probability of additional vulnerabilities being exploited. * Minor non-compliance with respect to some of the recommended controls defined in the organization’s policies and other legal, regulatory and statutory regulations and standards. |
|  | Very Low | * It will have negligible or no effect on security posture and brand value of the organization * Has negligible or no effect on critical services and operations of EAG / * Negligible amount of sensitive information stored or processed is compromised |

**Note:** Highlight the areas that correspond to the risk ratings assigned to the observed security issues or findings.