

## InfoSec - Vendor Security Assessment (VSA) Summary Report

**Third party:** Grabtaxi Holdings Pte Ltd  
**Scope of engagement:** Fraud Suite - GrabDefence Rule Engine  
**Assessment date:** 2 April - 15 April 2024  
**PIC Third Party:** Authorization Kumar Mishra;  
**BO Superbank:** Hapsoro Adi Permana [i.com](#)

The InfoSec team has examined the high level security posture of the third party based on the scope of engagement accordingly and summarized the following:

### Assessment result via questionnaires:



No	Aspect	Observation / Risk Description	Risk Level	Recommended Remediation Plan & Corrective Action	Status
1	Web Application Security	Multi Factor Authentication mechanism pending.	<b>Low</b>	Vendor to have the capability and will be integrated to JumpCloud to further safeguard user credentials used by Superbank.	<b>Closed</b>
2	Web Application Security	Secure communication protocol pending.  [HTTP Strict Transport Security (HSTS) not enforced. Strict Transport Security is an HTTP response header that tells clients to initiate connections over HTTPS only.]	<b>Low</b>	Additional checks to be performed: [Accessed domain Griffin: ] [Accessed domain OnePortal: ]  SSL certificate has not expired. SSL is supported for this site. With HSTS enforced, people browsing this site are less susceptible to man-in-the-middle attacks. All HTTP requests are redirected to HTTPS.	<b>Closed</b>
3	Web Application Security	Independent third-party SFTP (e.g. penetration testing) on the scope of	-	-	-

No	Aspect	Observation / Risk Description	Risk Level	Recommended Remediation Plan & Corrective Action	Status
		engagement <b>pending validation</b> .			
4	Security & Privacy Programs	No deficiency noted.	-	-	-

**Notes:**

- Oneportal: Is a web app which allows GD product users to visualize different fraud signals, sanctions and other information.
- Griffin (rule-editor): another web app, which allows for writing rules which works on variety of data points and generally enabling Policy creation and enforcement.
- xx
  - xx

**Supporting Documents :**

-  GrabDefence March 2024 - upguard-questionnaire-Superbank Security Questionnaire-Super Bank Indonesia\_response.xlsx
-  InfoSec Security Assessment - Grab Defense

**Risk Matrix**

Risk Level	Description
<b>High</b>	<ul style="list-style-type: none"><li>• Vendor has major security concerns (non-compliance)</li><li>• Unacceptable risk to overall security, privacy, and operations - there are no sufficient evidence to demonstrate expected information security controls are in place</li><li>• High impact to Superbank operational (downtime)</li><li>• Risk acceptance approval is required to proceed further</li></ul>
<b>Medium</b>	<ul style="list-style-type: none"><li>• Vendor has minor security concerns</li><li>• Acceptable medium risks to overall security, privacy, and operations</li><li>• Medium impact to Superbank operational (downtime)</li><li>• Risk acceptance approval may be required to proceed further</li></ul>
<b>Low</b>	<ul style="list-style-type: none"><li>• Vendor has minor or no security concerns</li><li>• Small risks to overall security, privacy, and operations</li><li>• No impact to Superbank operational (downtime)</li><li>• Risk acceptance approval is not required to proceed further</li></ul>