### Security

#### Access Control

##### **Authentication**

* Solution must support authentication via [-AD | -ADFS | -Azure AD | -Azure B2B | -OKTA | -Kerberos | -SAML2].
* Solution must support single sign on.
* Solution must support two-factor authentication.

##### **Authorization**

* Solution must grant access to users based on roles (RBAC).

##### **Data Isolation & Quarantine**

* Sensitive Data must be accessed only by privileged users and through authenticated channels.
* Solution must support data encryption at rest using [ -HSMs | -database file encryption | -database column encryption | -storage encryption | -disk encryption] without affecting performance.
* Solution must support data tokenization, or any other form of data privacy protection methods.
* For cloud solutions/services, (tenant) data must be logically or physically isolated/segregated from other customers’ data.
* Solution should support Microsoft CASB through APIs or CAAC for file labeling and/or protection.

#### Integrity

##### **System & Communication Security**

* Database connectivity credentials, passwords, keys, or any other restricted information/data must not be stored in plain text.
* Solution must support strong algorithms and key sizes (such as AES 256) for symmetric encryption use cases (if applicable).
* Data must be accessible only through service layers. Direct data access should not be allowed e.g. DB links.
* Solution must support encryption in transit using TLS 1.2.
* Cloud-based solutions/services must be protected against general and web attacks via [ -Intrusion Prevention System | -WAF | -DDOS protection] and must provide -application security logging and monitoring.
* All systems and components must be configured and developed securely (hardened / locked down).

#### Audit & Accountability

##### **Audit Trail**

* Audit trails exist for user management and administrator activities.
* Audit trails exist for all business transactions performed in the system. User Information & timestamp is a must.
* Auditing must be enabled for all transactions. In additional to the audit context data, following information is required with each audit << created by>> <<last modified by>> <<created date & time>> <<last modified date & time>>.
* Original values as well as new values must be captured in audit logs in key transactions (if applicable).
* Personal, credentials and other confidential information must not be saved in log files.
* Access of sensitive information must be tracked through Audit logs.

##### **System/Transaction Logs**

* Number of Users logging attempts (successful & failure) must be logged
* Transaction timestamps must be logged and enable tracing the supplier latency & processing time.
* Interface related transactions and exceptions must be logged in transaction logs with transaction details.

#### **SOC Integration**

* Solution should be integrated with AlFuttaim Security Operations Centers and integration Log entries must contain:
  + The name of the Application/system (on which the change was done) and its IP address.
  + The date and time of the log entry
  + The date and time of the event.
  + The true client IP address of the client system which triggered the event.
  + User ID that triggered the event.
  + Successful and failed changes done to the Application/system.
  + Success and failure login attempts.
  + Values before and after the change (if applicable).

#### **Security Assurance**

* All vulnerability assessment and/or penetration test findings reported and/or conducted by AlFuttaim, any 3rd party, or independent entities must be mitigated.
* Cloud providers must undergo a 3rd party risk assessment and must provide a response to a cloud security questionnaire.
* All security testing use cases and requirements must be successfully met

#### Interfaces

* Secure APIs
* Solution APIs must support:
  + Certificates or secure token-based authentication
  + oAuth2 for authorization
  + IP whitelisting to allow connection only from known source
  + API calls must not have direct connectivity to/from AlFuttaim network and must be inspected for intrusions, contracts validity, rate limiting, etc.

#### Compliance

* All assets (including technology, processes & people) within scope shall adhere to applicable industry, national & international laws and regulations such as GDPR, PCI-DSS, SWIFT, etc.