Hosted Solution Security Questionnaire

Intent

The Ministry of Finance, Banking and Postal Services (MOFBPS) of the Marshall Islands has an obligation to protect the confidentiality of taxpayer and government data. This obligation is enshrined in law.

The intent of the questionnaire is to understand the cybersecurity practices and controls that have been or will be implemented for any cloud-based solution or solution hosted outside of the Government of the Marshall Islands computer networks, that has been proposed by a tenderer.

If you are proposing an on-premises solution to be hosted by the Government of the Marshall Islands, you do not need to complete this questionnaire.

Questions:

Personnel security

DOFBPS seeks to mitigate threats from malicious internal actors (trusted insiders).
What processes and procedures are in place for hiring, managing and terminating employees and contractors who will be involved in the maintenance or management of the proposed solution.
Processes and procedures may include but are not limited to:

- Identity proofing/pre-employment screening
- Qualification checks
- Previous employment checks
- Police checks
- Employee obligations
- Separation activities

Potential Evidence

- Internal policy document detailing how employees maintain confidentiality of enterprise information,
- Process descriptions detailing pre-employment screening and separation procedures, or
- Sample contracts detailing conditions of employment

Tenderer's Claims / Evidence

Encryption in transit

DOFBPS seeks to protect the confidentiality and integrity of taxation related information in transit.
Provide evidence that your product or service utilises TLS 1.2 or another NIST approved cryptographic algorithm and/or protocol.

Potential Evidence

A screenshot of:

- SSL Labs report

Tenderer's Claims / Evidence

Encryption at rest

DOFBPS seeks to protect taxation related information from unauthorised access.
You may apply encryption at the disk, container, application or database level. Encryption at rest should follow NIST or similar guidelines for approved cryptographic algorithms and protocols.

Potential Evidence

Evidence could include:

- Screenshot showing encryption enabled at the database or disk level with the type of encryption at rest being used
- When using 'out of the box' encryption a licensing agreement or screenshot showing 'out of the box' encryption at rest enabled
- If using the infrastructure of a cloud provider to encrypt data at rest, an invoice or contract agreement could be provided or screenshot from within the cloud environment showing encryption enabled

Where encryption at rest is not viable, evidence must be provided of a full range of data protection controls. These must include:

- User/system (service account) access control (including authentication and authorisation) and active logging and monitoring protocols
- Intrusion Detection System/Intrusion Prevention System
- Internal employee screening or vetting
- Isolation of/and handling procedures for sensitive data including restrictions such as 'need to know' principles

Tenderer's Claims / Evidence

Encryption key management

MOFBPS seeks to minimise the risks of compromised encryption keys.

You need to demonstrate that a policy or process in place to govern the use of your encryption keys.

Potential Evidence

Your key management plan should cover the generation, distribution, storage, access, renewal, revocation, rotation, length and complexity of keys, recovery, archiving and destruction of compromised encryption keys.

Tenderer's Claims / Evidence

Audit logging

MOFBPS seeks to ensure traceability of access and actions within the MOFBPS tenancy and any shared capabilities.

Audit logging should include both application level (access logs) and event-based actions.

MOFBPS would like confidence the tenderer is able to access or supply the logs on the occurrence of a security event where further investigation of the data is required.

Potential Evidence

- Sample of a dummy audit log in CSV format
- A data dictionary that describes the data attributes and maps against key audit log components

Tenderer's Claims / Evidence

Certification (Independent or self-assessment)

DOFBPS seeks a level of assurance that you have robust security practices in place across your organisation. This may be achieved by way of an independent or self-assessment against one of the below standards:

- ISO/IEC 27001
- OWASP ASVS3.0 or
- SOC2

You may use an alternative security standard or internal framework if you feel it would be more suitable for your circumstances.

The DOFBPS are not prescribing which of the above methods you should use. The choice of what standard should be made on the basis of suitability to your organisation.

We don't expect you to be fully compliant with the complete range of controls of your chosen standard. The controls that you should be compliant with will be dependent on your organisation's operating model and the architecture of your product.

We also acknowledge there may be areas where you are unable to demonstrate compliance with particular controls. In these scenarios you will be required to offer supporting commentary to substantiate the non-compliance.

Potential Evidence

- An independent certification
- A self-assessment spreadsheet/report
- Existing IT Security Management framework and policy document

Tenderer's Claims / Evidence

Security monitoring practices

DOFBPS seeks to ensure hosted solutions can detect and respond to cyber-attacks, channel misuse and business threats. Where relevant you need to be able to demonstrate that you scan your environment for threats and that you take appropriate action where you detect anomalies.

Potential Evidence

Network / infrastructure layer - relevant combinations of:

- screenshots of an intrusion detection system or firewall that generates alerts.
- photos of your security information and event management dashboard
- If leveraging off a cloud provider you can provide either an invoice or screenshot from within the environment showing the type of monitoring captured.

Application layer – relevant combinations of:

- screenshots of the function page in the application, and
- reports from the backend system.

Transaction (data) layer – relevant combinations of:

- reports from the backend system
- screenshots of an anomaly detection system.

Tenderer's Claims / Evidence