

# Third-Party Assessment

## Date: 29th November 2023

# Risk Summary

The MOP Team has an acceptable level of security maturity but with some areas of improvement. The MOP team has demonstrated commitment to the security of their services.  
  
Strong track record of transparency and maintaining the security of their product/service and their supply chain.

Overall the risk is low, and the impact of a vendor compromise is low due to the classification & volume of records

Based on the review of responses to the security questionnaire, and the review of the provided documentation, there is reasonable assurance that the MOP team’s website has satisfactory information security controls.

## Risk Finding Count

| Risk Rating | Count |
| --- | --- |
| Significant | 0 |
| Major | 0 |
| Moderate | 0 |
| Minor | 0 |

# 

## Engagement Scope

**In Scope**

This TPA covers the following:

* General security governance assessment of the MOP teams security maturity;
* Focused assessment on the security controls and mechanisms that the vendor has in place, to protect customer and corporate data.

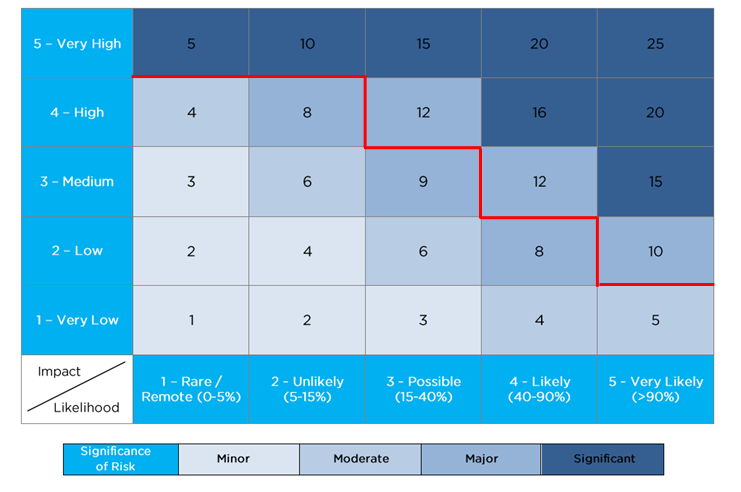
Control Standards Alignment

| **Control Group** | **Control Effectiveness** |
| --- | --- |
| Application Development | Effective |
| Asset Management & Configuration Management | Effective |
| Boundary Defence | Effective |
| Cyber Resilience | Effective |
| Data & Information Protection | Effective |
| Education and Awareness | Not Relevant |
| Endpoint Security & Malware Defences | Not Relevant |
| Identity & Access Management | Effective |
| Incident & Problem Management | Effective |
| IT Change Management | Effective |
| Network & Wireless Security | Not Relevant |
| Platform & Cloud Security | Effective |
| Security Operations & Vulnerability Management | Effective |
| Service Design & Technology Resilience | Effective |
| Physical Security | Effective |
| Third Party Management | Effective |
| Security Governance | Effective |

# Risk Assessment

| Security Domain | | Observation & Recommendation |
| --- | --- | --- |
| Application Development | | No gaps observed |
| Asset Management & Configuration Management | | No gaps observed |
| Cyber Resilience | | No gaps observed |
| Data & Information Protection | | No gaps observed |
| Education and Awareness | | No gaps observed |
| Endpoint Security & Malware Defences | | No gaps observed |
| Identity & Access Management | | No gaps observed |
| Incident & Problem Management | | No gaps observed |
| IT Change Management | | No gaps observed |
| Network & Wireless Security | | No gaps observed |
| Platform & Cloud Security | | Gaps observed  Unable to confirm the location of the data.  Unable to confirm if data is encrypted.  Cloud-based storage is not protected by MFA or 2FA |
| Security Operations & Vulnerability Management | | Gaps observed  Unable to confirm regular security patches |
| Service Design & Technology Resilience | | No gaps observed |
| Physical Security | | No gaps observed |
| Third Party Management | | No gaps observed |
| Security Governance | | No gaps observed |

## Risk Rating[[1]](#footnote-0)

****

# Key Considerations

Below are the key points discussed while performing the TPA – Some of these were not mentioned in the scoping documents but understood will be incorporated during the delivery/implementation.

* {insert any assumptions or considerations identified during the BO interviews}
* Risks are assessed based on Bupa’s Risk Management framework.
* All risks identified are based on Residual Risk which is the risk position that remains if the project doesn’t implement the recommended mitigating / compensating controls outlined in this document.
* The full scope of the Bupa IS Schedule will apply to any MSA entered into with the vendor.

# Document Revision

| Date | Version | Author | Comments |
| --- | --- | --- | --- |
|  | V0.1 | Theodore Savvidis | First Draft |
|  | V0.2 |  | Peer review |
|  | V1.0 | Theodore Savvidis | Final |

1. [↑](#footnote-ref-0)