**Rating Summary:**

Vendor has "Mostly Effective" controls and "Medium" residual risk making it "Satisfactory" to work with Client.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| {{INHERENT RISK}} | |  | {{CONTROL EFFECTIVENESS}} | |  | {{RESIDUAL RISK}} | | |
| INHERENT RISK | |  | CONTROL EFFECTIVENESS | |  | RESIDUAL RISK | | |
|  |  |  |  |  |  |  |  | |
| Data **{{INHERENT RISK}}** | Confidential | | Control testing metrics | {{Control testing metrics}} |  | Inherent Risk | {{INHERENT RISK}} | |
| Saas | Yes |  | Total gaps | {{Total gaps}} |  | Control Effectiveness | {{CONTROL EFFECTIVENESS}} | |
| External Access | Yes |  | Critical gaps | {{Critical gaps}} |  |  |  | |
| Customer Data | Yes |  |  |  |  |  |  | |
| Fourth Party Access | Yes |  |  |  |  |  |  | |
| Application Dependability | No |  |  |  |  |  |  | |
|  | | | | | | | |
|  | | | | | | | |

For additional details on the values, please visit the following link: <https://beaconer.io/resources>

**Control Testing Metrics:**

This Section provides the High level results of the assessment based on a maturity model and completeness of the control implementation.

|  |  |  |  |
| --- | --- | --- | --- |
| {{Overall Score}} | {{HIGH}} | {{MEDIUM}} | {{LOW}} |
| Overall Score | HIGH | MEDIUM | LOW |
|  |  |  |  |
|  | FAILED IN-SCOPE CONTROL |  | FAILED CRITICAL CONTROL |
|  | {{FAILED IN-SCOPE CONTROL}} |  | {{FAILED CRITICAL CONTROL}} |
|  |  |  |  |
|  |  |  |  |
|  | High Risk (0-40%) | Medium Risk (40 - 70%) | Low (70-95%) |

**Domain Summary:**

This Section provides the High-level results of the assessment based on a maturity model and completeness of the control implementation.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Access Control** | {{Domain Summary Access Control}} |  |  |  |  |
|  |  |  |  |  |  |
| **Access Program** | | **Authentication** | | **Passwords** | |
| **Control** | **Response** | **Control** | **Response** | **Control** | **Response** |
| Program approved & communicated | Yes | MFA deployed | Yes | Password sharing prohibited | Yes |
| Regular access review for all | Yes | Application supports customer SSO | Yes | Password Policy | Yes |
| Process to request approval for access | Yes | Unique IDs required | Yes | Password are salted & hashed at storage | Yes |
| Segregation of duties | Yes | Principle of lease privilege | Yes |  |  |
| IDs are auto terminated on last day | Yes |  |  |  |  |
| Controls for Corporate Email on Personal Phones | Yes |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Application Security** | {{Domain Summary Application Security}} |  |  |  |  |
|  |  |  |  |  |  |
| **API Security** | | **App Sec Program** | | **Secure Coding** | |
| **Control** | **Response** | **Control** | **Response** | **Control** | **Response** |
| Formal API Security program | Yes | Program approved & communicated | Yes | WAF implemented for external app | Yes |
| Data encrypted in transit within API | Yes | Software security training to Developers | Yes | Production Data used in testing | Yes |
| APIs are managed using standard API Integration platform | Yes | Industry Best practices used for Coding | Yes | Static Code Analysis testing (SAST) performed | Yes |
| API access logged & monitored | Yes | Application Change control exist | Yes | Dynamic Code Analysis testing (DAST) performed | Yes |
| Only secure authentication is used for APIs | Yes | Security testing done before moving to Prod | Yes | SCA (Security composition Analysis) performed | Yes |

**Privacy Impact Assessment:**

This section provides the High level results of the Privacy Impact assessment based on the Project scope and its privacy requirements.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| {{Privacy Impact Assessment INHERENT RISK}} |  | {{Privacy Impact Assessment CONTROL EFFECTIVENESS}} |  | {{Privacy Impact Assessment RESIDUAL RISK}} |
| INHERENT RISK |  | CONTROL EFFECTIVENESS |  | RESIDUAL RISK |

|  |  |  |  |
| --- | --- | --- | --- |
| {{Privacy Impact Assessment Privacy Score}} |  |  |  |
| Privacy Score | TESTED CONTROL |  | CRITICAL CONTROL |
|  | {{Privacy Impact Assessment TESTED CONTROL}} |  | {{Privacy Impact Assessment CRITICAL CONTROL}} |
|  |  |  |  |
|  | FAILED CONTROL |  | CRITICAL FAILED |
|  | {{Privacy Impact Assessment FAILED CONTROL}} |  | {{Privacy Impact Assessment CRITICAL FAILED}} |
|  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Control Tested** |  |  |  |  |
|  |  |  |  |  |
| Privacy Program including Policy | Yes |  | Strict Controls to protect PI/SPI | Yes |
| Privacy Impact assessment | Yes |  | Clean history on Privacy complaints or incidents | Yes |
| Privacy Awareness Training | Yes |  | SPI/PHI Masked/Anonymized/coded | Yes |
| PI/SPI destroyed or erased at the end | Yes |  | Data Residency controls | Yes |
| Consent from Data Subject | Yes |  | PI/SPI Encrypted with AES 256 or TLS 1.2 | Yes |
| Comply with DSARs (Data Subject Access Requests) | Yes |  | PI/SPI are not used in the test environment | Yes |
| Fourth party access to PI/SPI | Yes |  | Logging & monitoring for PI Data | Yes |
| Fourth Party Privacy assessment | Yes |  | AI does not use PI/SPI for decision making | Yes |

Control Gaps:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Domain** | **Issues Identified** | **Severity (High/Medium/Low)** | **Risk** | **Counter Measure** |
| Access Control | Password rotation for users every 6 months | Medium | Credential brute-force exposure | Reduce to 90 days rotation or enforce universal MFA |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |