**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 | 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%}} | {{Control Testing Metrics HIGH Value}} | {{Control Testing Metrics MEDIUM Value}} | {{Control Testing Metrics LOW Value}} |
| 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 | {{Domain Summary Access Control Program approved and communicated Yes or No}} | MFA deployed | {{Domain Summary Authentication MFA deployed Yes or No}} | Password sharing prohibited | {{Domain Summary Passwords Password sharing prohibited Yes or No}} |
| Regular access review for all | {{Domain Summary Access Control Regular access review for all Yes or No}} | Application supports customer SSO | {{Domain Summary Authentication Application supports customer SSO Yes or No}} | Password Policy | {{Domain Summary Passwords Password Policy Yes or No}} |
| Process to request approval for access | {{Domain Summary Access Control Process to request approval for access Yes or No}} | Unique IDs required | {{Domain Summary Authentication Unique IDs required Yes or No}} | Password are salted & hashed at storage |  |
| Segregation of duties | {{Domain Summary Access Control Segregation of duties Yes or No}} | Principle of lease privilege | {{Domain Summary Authentication Principle of least privilege Yes or No}} |  |  |
| IDs are auto terminated on last day | {{Domain Summary Access Control IDs are auto terminated on last day Yes or No}} |  |  |  |  |
| Controls for Corporate Email on Personal Phones | {{Domain Summary Access Control Controls for Corporate Email on Personal Phones Yes or No}} |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Application Security** | {{Domain Summary Application Security %}} |  |  |  |  |
|  |  |  |  |  |  |
| **API Security** | | **App Sec Program** | | **Secure Coding** | |
| **Control** | **Response** | **Control** | **Response** | **Control** | **Response** |
| Formal API Security program | {{Domain Summary API Security Formal API Security program Yes or No}} | Program approved & communicated | {{Domain Summary Application Security Program approved and communicated Yes or No}} | WAF implemented for external app | {{Domain Summary Secure Coding WAF implemented for external app Yes or No}} |
| Data encrypted in transit within API | {{Domain Summary API Security Data encrypted in transit within API Yes or No}} | Software security training to Developers | {{Domain Summary Application Security Software security training to Developers Yes or No}} | Production Data used in testing | {{Domain Summary Secure Coding Production Data used in testing Yes or No}} |
| APIs are managed using standard API Integration platform | {{Domain Summary API Security APIs are managed using standard API Integration platform Yes or No}} | Industry Best practices used for Coding | {{Domain Summary Application Security Industry Best practices used for Coding Yes or No}} | Static Code Analysis testing (SAST) performed | {{Domain Summary Secure Coding Static Code Analysis testing (SAST) performed Yes or No}} |
| API access logged & monitored | {{Domain Summary API Security API access logged and monitored Yes or No}} | Application Change control exist | {{Domain Summary Application Security Application Change control exist Yes or No}} | Dynamic Code Analysis testing (DAST) performed | {{Domain Summary Secure Coding Dynamic Code Analysis testing (DAST) performed Yes or No}} |
| Only secure authentication is used for APIs | {{Domain Summary API Security Only secure authentication is used for APIs Yes or No}} | Security testing done before moving to Prod | {{Domain Summary Application Security Security testing done before moving to Prod Yes or No}} | SCA (Security composition Analysis) performed | {{Domain Summary Secure Coding SCA (Security composition Analysis) performed Yes or No}} |

**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 Value}} |  | {{Privacy Impact Assessment CRITICAL CONTROL Value}} |
|  |  |  |  |
|  | FAILED CONTROL |  | CRITICAL FAILED |
|  | {{Privacy Impact Assessment FAILED CONTROL Value}} |  | {{Privacy Impact Assessment CRITICAL FAILED Value}} |
|  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Control Tested** |  |  |  |  |
|  |  |  |  |  |
| Privacy Program including Policy | {{Privacy Control Tested Privacy Program including Policy Yes or No}} |  | Strict Controls to protect PI/SPI | {{Privacy Control Tested Strict Controls to protect PI or SPI Yes or No}} |
| Privacy Impact assessment | {{Privacy Control Tested Privacy Impact assessment Yes or No}} |  | Clean history on Privacy complaints or incidents | {{Privacy Control Tested Clean history on Privacy complaints or incidents Yes or No}} |
| Privacy Awareness Training | {{Privacy Control Tested Privacy Awareness Training Yes or No}} |  | SPI/PHI Masked/Anonymized/coded | {{Privacy Control Tested SPI or PHI Masked Anonymized coded Yes or No}} |
| PI/SPI destroyed or erased at the end | {{Privacy Control Tested PI or SPI destroyed or erased at the end Yes or No}} |  | Data Residency controls | {{Privacy Control Tested Data Residency controls Yes or No}} |
| Consent from Data Subject | {{Privacy Control Tested Consent from Data Subject Yes or No}} |  | PI/SPI Encrypted with AES 256 or TLS 1.2 | {{Privacy Control Tested PI or SPI Encrypted with AES 256 or TLS 1.2 Yes or No}} |
| Comply with DSARs (Data Subject Access Requests) | {{Privacy Control Tested Comply with DSARs Data Subject Access Requests Yes or No}} |  | PI/SPI are not used in the test environment | {{Privacy Control Tested PI or SPI are not used in the test environment Yes or No}} |
| Fourth party access to PI/SPI | {{Privacy Control Tested Fourth party access to PI or SPI Yes or No}} |  | Logging & monitoring for PI Data | {{Privacy Control Tested Logging and monitoring for PI Data Yes or No}} |
| Fourth Party Privacy assessment | {{Privacy Control Tested Fourth Party Privacy assessment Yes or No}} |  | AI does not use PI/SPI for decision making | {{Privacy Control Tested AI does not use PI or SPI for decision making Yes or No}} |

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 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |