# Third-Party Risk Assessment Report

## Gaspar Labs

Vendor Tier

**TIER 2**

Annual

Overall Risk Score

**MODERATE**

Score: 8

Assessment Date: 4/24/2026

Assessment Type: Vendor Completed SIG

# Table of Contents

# Executive Summary

Vendor: Gaspar Labs

Assessment Date: 4/24/2026

| Vendor Tier | Overall Risk | Cert Coverage |
|---|---|---|
| TIER 2 | MODERATE | 75% |
| High | Score: 8 | 5 cert(s) |

## Assessment Overview

- SIG Questionnaire: SIG 2025 - 755 questions
- Domains Assessed: 21
- Overall Risk Score: 8 (MODERATE)
- Third-Party Rating: No third-party rating provided
- Selected Certifications: SOC 2 Type 2, ISO 27001, HITRUST CSF, ISO 27701, PCI-DSS
- Evidence Files: No evidence files uploaded

## High-Risk Domains

| Domain | Score | Rating |
|---|---|---|
| I. Application Management | 12 | HIGH |
| U. Server Security | 12 | HIGH |
| V. Cloud Services | 12 | HIGH |

## Recommendation

**CONDITIONAL APPROVAL - Proceed with standard monitoring**

## Recommended Actions

1. Schedule annual security review
2. Ensure contractual security requirements are documented
3. Address gaps in high-risk domains: I, U, V

# Vendor & Tiering Summary

## Vendor Information

| | |
|---|---|
| **Vendor Name** | Gaspar Labs |
| **Contact Name** | - |
| **Contact Email** | - |
| **Assessment Date** | 4/24/2026 |

HIGH

**TIER 2**

Access to important but non-catastrophic data or systems

## Additional Information

| | | | |
|---|---|---|---|
| **Primary Contact** | Carl Gaspar <email@carlgaspar.com> | **Secondary Contact** | - |

## Tiering Criteria

| Criteria | Selection |
|---|---|
| **Data Access Types** | PII (Personally Identifiable Information), Private/Internal Data |
| **Data Access** | Not selected |
| **Data Transfer Method** | API |
| **Identity and Access Type** | Service account / API key |

## Tier Definitions

| Tier | Risk Level | Assessment Frequency |
|---|---|---|
| **Tier 1** | Critical | Annual + Continuous Monitoring |
| **Tier 2** | High | Annual |
| **Tier 3** | Medium | Every 2 Years |
| **Tier 4** | Low | Every 2 Years |

## Third Party Rating

| Cyber Security Scan Score | Ransomware Susceptibility Index |
|---|---|
| - | - |

*No evidence provided*

# Domain Risk Overview

Assessment Type: Vendor Completed SIG

Total Domains: 21

**Risk Rating Guide**

| Range | Rating |
|---|---|
| 1 - 5 | LOW |
| 6 - 10 | MODERATE |
| 11 - 15 | HIGH |
| 16 - 25 | EXTREME |

Overall Risk Score

**8**

**MODERATE**

| ID | Domain | Crit | B.Imp | I.Adj | Imp | B.Lklhd | Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| A | Enterprise Risk Management | Medium | 3 | 0 | 3 | 2.4 | 2 | 6 |
| B | Nth Party Management | Medium | 3 | 0 | 3 | 3.0 | 3 | 9 |
| C | Information Assurance | Medium | 3 | 0 | 3 | 2.4 | 2 | 6 |
| D | Asset and Info Management | High | 4 | 0 | 4 | 2.4 | 2 | 8 |
| E | Human Resources Security | High | 4 | 0 | 4 | 2.4 | 2 | 8 |
| F | Physical and Environmental | High | 4 | 0 | 4 | 2.4 | 2 | 8 |
| G | IT Operations Management | High | 4 | 0 | 4 | 2.4 | 2 | 8 |
| H | Access Control | High | 4 | 0 | 4 | 2.4 | 2 | 8 |
| I | Application Management | High | 4 | 0 | 4 | 3.0 | 3 | 12 |
| J | Cybersecurity Incident Mgmt | High | 4 | 0 | 4 | 2.4 | 2 | 8 |
| K | Operational Resilience | High | 4 | 0 | 4 | 2.4 | 2 | 8 |
| L | Compliance and Ops Risk | Medium | 3 | 0 | 3 | 2.4 | 2 | 6 |
| M | Endpoint Device Security | High | 4 | 0 | 4 | 2.4 | 2 | 8 |
| N | Network Security | High | 4 | 0 | 4 | 2.4 | 2 | 8 |
| O | Environ, Social, Gov (ESG) | Medium | 3 | 0 | 3 | 4.5 | 3 | 9 |
| P | Privacy | High | 4 | 0 | 4 | 2.4 | 2 | 8 |
| R | AI Governance | Medium | 3 | 0 | 3 | 4.5 | 3 | 9 |
| S | Supply Chain Risk Mgmt | Medium | 3 | 0 | 3 | 3.0 | 3 | 9 |
| T | Threat Management | High | 4 | 0 | 4 | 2.4 | 2 | 8 |
| U | Server Security | High | 4 | 0 | 4 | 3.0 | 3 | 12 |
| V | Cloud Services | High | 4 | 0 | 4 | 3.0 | 3 | 12 |

*• Criticality: Based on Vendor Tier classification*
*• Impact: Derived from Criticality - Critical=5, High=4, Medium=3, Low=2, N/A=1*
*• Likelihood: Based on Certifications - 5=Almost Certain, 4=Likely, 3=Possible, 2=Unlikely, 1=Rare*
*• I. Adj.: Manual adjustment of ±1 for Impact*
*• Risk Score: Impact × Likelihood*

# Certifications & Coverage Reference

Average Coverage: 75% (19 of 21 domains covered)

## Vendor Certifications

| Certification | Description | Status |
|---|---|---|
| CSA STAR | Cloud Security Alliance Security Trust Assurance and Risk | No |
| Cyber Essentials | UK government-backed certification for basic cyber hygiene | No |
| FedRAMP | Federal Risk and Authorization Management Program for cloud services | No |
| GDPR Compliance | EU General Data Protection Regulation compliance attestation | No |
| HIPAA Compliance | Health Insurance Portability and Accountability Act compliance | No |
| HITRUST CSF | Comprehensive framework integrating 50+ standards including HIPAA, NIST, ISO | Yes |
| ISO 27001 | International standard for Information Security Management System (ISMS) | Yes |
| ISO 27701 | Privacy extension to ISO 27001 for Privacy Information Management | Yes |
| NIST 800-53 | Security and Privacy Controls for Federal Information Systems | No |
| NIST CSF | NIST Cybersecurity Framework for critical infrastructure | No |
| PCI-DSS | Payment Card Industry Data Security Standard | Yes |
| SOC 2 Type 2 | AICPA Trust Services Criteria attestation (Security, Availability, Confidentiality) | Yes |

## Coverage Reference

| Certification | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | R | S | T | U | V |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CSA STAR | 50% | 55% | 70% | 70% | 55% | 50% | 65% | 75% | 70% | 70% | 70% | 75% | 60% | 70% | - | 60% | - | 60% | 65% | 70% | 85% |
| Cyber Essentials | - | - | 40% | 35% | 30% | 25% | 30% | 50% | 40% | 30% | 25% | 40% | 50% | 55% | - | 20% | - | - | 40% | 45% | 35% |
| FedRAMP | 70% | 65% | 85% | 80% | 75% | 75% | 80% | 90% | 80% | 85% | 80% | 90% | 75% | 85% | - | 70% | - | 70% | 75% | 80% | 95% |
| GDPR Compliance | 30% | 40% | 50% | 60% | 45% | 30% | 30% | 50% | 30% | 40% | 30% | 70% | 30% | 35% | - | 95% | - | 40% | 30% | 30% | 30% |
| HIPAA Compliance | 50% | 45% | 70% | 75% | 60% | 55% | 55% | 75% | 50% | 70% | 60% | 80% | 60% | 65% | - | 90% | - | 50% | 55% | 60% | 50% |
| HITRUST CSF | 80% | 75% | 90% | 90% | 85% | 80% | 80% | 90% | 75% | 85% | 80% | 90% | 80% | 85% | - | 95% | - | 75% | 80% | 75% | 75% |
| ISO 27001 | 85% | 70% | 90% | 85% | 80% | 75% | 70% | 80% | 65% | 75% | 70% | 85% | 65% | 70% | - | 60% | - | 70% | 70% | 65% | 60% |
| ISO 27701 | 40% | 45% | 60% | 65% | 50% | 40% | 40% | 55% | 40% | 45% | 40% | 60% | 40% | 45% | - | 95% | - | 45% | 40% | 40% | 40% |
| NIST 800-53 | 85% | 75% | 90% | 85% | 80% | 80% | 80% | 90% | 80% | 85% | 85% | 90% | 80% | 85% | - | 70% | - | 75% | 80% | 80% | 80% |
| NIST CSF | 75% | 60% | 85% | 75% | 70% | 65% | 70% | 80% | 70% | 80% | 75% | 80% | 70% | 75% | - | 55% | - | 65% | 75% | 70% | 65% |
| PCI-DSS | - | - | 50% | 60% | 55% | 60% | 55% | 85% | 75% | 65% | 50% | 70% | 80% | 90% | - | 50% | - | - | 70% | 75% | 50% |
| SOC 2 Type 2 | 60% | 50% | 75% | 70% | 65% | 65% | 75% | 85% | 60% | 75% | 80% | 85% | 60% | 75% | - | 65% | - | 55% | 65% | 70% | 70% |

# Calculated Coverage Summary

Selected Certifications: SOC 2 Type 2, ISO 27001, HITRUST CSF, ISO 27701, PCI-DSS

**Domains Covered: 19 of 21**

| ID | Domain | Coverage | Contributing Certifications |
|---|---|---|---|
| A | Enterprise Risk Management | 85% | ISO 27001 |
| B | Nth Party Management | 75% | HITRUST CSF |
| C | Information Assurance | 90% | ISO 27001, HITRUST CSF |
| D | Asset and Info Management | 90% | HITRUST CSF |
| E | Human Resources Security | 85% | HITRUST CSF |
| F | Physical and Environmental | 80% | HITRUST CSF |
| G | IT Operations Management | 80% | HITRUST CSF |
| H | Access Control | 90% | HITRUST CSF |
| I | Application Management | 75% | HITRUST CSF, PCI-DSS |
| J | Cybersecurity Incident Mgmt | 85% | HITRUST CSF |
| K | Operational Resilience | 80% | SOC 2 Type 2, HITRUST CSF |
| L | Compliance and Ops Risk | 90% | HITRUST CSF |
| M | Endpoint Device Security | 80% | HITRUST CSF, PCI-DSS |
| N | Network Security | 90% | PCI-DSS |
| O | Environ, Social, Gov (ESG) | - | - |
| P | Privacy | 95% | HITRUST CSF, ISO 27701 |
| R | AI Governance | - | - |
| S | Supply Chain Risk Mgmt | 75% | HITRUST CSF |
| T | Threat Management | 80% | HITRUST CSF |
| U | Server Security | 75% | HITRUST CSF, PCI-DSS |
| V | Cloud Services | 75% | HITRUST CSF |

# Additional Evidence Files

*No evidence files uploaded*

# Questions Detail

## Scoring Guide

| | | | | | |
|---|---|---|---|---|---|
| **Impact Score** | 5=Critical | 4=High | 3=Medium | 2=Low | 1=N/A |
| **Likelihood Score** | 5=Almost Certain | 4=Likely | 3=Possible | 2=Unlikely | 1=Rare |
| **Risk Score** | 16-25 Extreme | 11-15 High | 6-10 Moderate | 1-5 Low | |

## A. Enterprise Risk Management

***Domain Baselines - Criticality: Medium | Impact: 3 | Likelihood: 2***

**Domain Risk: 6**

Evidence: -

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| A.1 | Is there a formalized risk governance policy approved by management th... | Yes | Gaspar Labs's risk governance ... | 3 | 2.4 | 0 | 2.4 | 6 |
| A.1.1 | Does the risk governance program include risk management policies, pro... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| A.1.2 | Does the risk governance program include range of assets to include: p... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| A.1.3 | Does the governing body define the accountabilities of management and ... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| A.1.4 | Is the risk governance program approved by senior management and/or bo... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| A.1.5 | Is training provided to employees regarding risk expectations and thei... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| A.1.6 | Does the organization's risk management program include processes that... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| A.2 | Are there Subject Matter Experts (SMEs) and/or groups assigned to asse... | Yes | Members of Gaspar Labs's IMS C... | 3 | 2.4 | 0 | 2.4 | 6 |
| A.3 | Is there a formalized Risk Assessment process that requires identifyin... | Yes | Gaspar Labs conducts a risk as... | 3 | 2.4 | 0 | 2.4 | 6 |
| A.3.1 | Does the risk assessment process identify and monitor inherent and res... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| A.3.2 | Are risks to critical processes and entities reassessed annually? | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| A.3.3 | Does the organization have a process in place for documenting and appr... | Yes | Gaspar Labs performs an annual... | 3 | 2.4 | 0 | 2.4 | 6 |
| A.3.4 | Is there a formal process in the risk management program to identify, ... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| A.4 | Does the Enterprise Risk Management program include measures for defin... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |

## B. Nth Party Management

***Domain Baselines - Criticality: Medium | Impact: 3 | Likelihood: 3***

**Domain Risk: 9**

Evidence: -

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| B.1 | Is there a third party risk management program that is reviewed and ap... | Yes | Gaspar Labs conducts a risk as... | 3 | 2.5 | 0 | 2.5 | 9 |
| B.1.1 | Are there established third-party risk management standards or procedu... | Yes | Yes, Gaspar Labs has a policy ... | 3 | 2.5 | 0 | 2.5 | 9 |
| B.1.2 | Have policies, standards, and procedures for implementing the third pa... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| B.2 | For all organizational entities (e.g., vendor's vendors, subcontractor... | Yes | All Gaspar Labs sub-processors... | 3 | 2.5 | 0 | 2.5 | 9 |
| B.2.1 | Does the third-party risk management program require Confidentiality a... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| B.2.2 | Do third-party contracts include all applicable privacy and security c... | Yes | Yes, Gaspar Labs conducts a ri... | 3 | 2.5 | 0 | 2.5 | 9 |

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| B.2.3 | Do third-party party contracts include incident and data breach notifi... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| B.2.4 | Does the third party risk management program include creating and main... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| B.2.5 | Does the third party risk management program have a governing body acc... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| B.2.6 | Are the activities of third party personnel monitored for potential se... | Yes | Gaspar Labs requires subproces... | 3 | 2.5 | 0 | 2.5 | 9 |
| B.2.7 | Does the third party risk management program include definition of req... | Yes | Suppliers are monitored by the... | 3 | 2.5 | 0 | 2.5 | 9 |
| B.2.7.1 | Does the third party risk management program include the definition of... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| B.2.8 | Does the third party risk management program include definition and a ... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| B.2.9 | Are third-parties or service providers evaluated for reassessment when... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| B.2.10 | Does the third party risk management program include assessments perfo... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| B.2.11 | Does the third party risk management program include requirements to r... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| B.2.12 | Does the third party risk management program require notification for ... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| B.2.13 | Does the third party risk program require notification by each party o... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| B.2.14 | Does the third party risk management program require background checks... | Yes | Gaspar Labs requires subproces... | 3 | 2.5 | 0 | 2.5 | 9 |
| B.2.15 | Does the third party risk management program include an assigned indiv... | Yes | Suppliers are monitored by the... | 3 | 2.5 | 0 | 2.5 | 9 |

## C. Information Assurance

***Domain Baselines - Criticality: Medium | Impact: 3 | Likelihood: 2***

**Domain Risk: 6**

Evidence: -

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| C.1 | Is there a documented, approved cybersecurity risk management policy c... | Yes | Gaspar Labs has a Information ... | 3 | 2.4 | 0 | 2.4 | 6 |
| C.1.2 | Has the organization determined and documented the scope of the inform... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| C.1.3 | Does the information security policy have clearly defined and measurab... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| C.1.4 | Are information security policies, standards, and procedures based on ... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| C.1.5 | Does the organization have a documents and records management program ... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| C.1.6 | Does the information security program establish requirements for the p... | Yes | Gaspar Labs has implemented te... | 3 | 2.4 | 0 | 2.4 | 6 |
| C.2 | Has senior management designated and communicated a qualified owner (e... | Yes | Gaspar Labs's internal securit... | 3 | 2.4 | 0 | 2.4 | 6 |
| C.2.1 | Does the Chief Information Security Officer (CISO) or designated owner... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| C.2.2 | Is there a management-approved information security process for handli... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| C.2.3 | Does the information security program define and set objectives and pr... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| C.3 | Does senior management clearly identify and communicate the roles and ... | Yes | Gaspar Labs has a Human Resour... | 3 | 2.4 | 0 | 2.4 | 6 |
| C.3.4 | Have any of the Information Security and IT processes been outsourced? | No | Gaspar Labs does not outsource... | 3 | 2.4 | 0 | 2.4 | 6 |
| C.3.5 | Do the information security policies and procedures include requiremen... | Yes | Gaspar Labs has a Human Resour... | 3 | 2.4 | 0 | 2.4 | 6 |
| C.4 | Is there a documented risk assessment process for information security... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| C.4.1 | Does the information security assessment process include residual risk... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| C.4.2 | Does the information security risk assessment process address the risk... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| C.4.3 | Does assessing infosec risks involve identifying owners, analyzing ris... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| C.5 | Do all projects involving systems, applications, and platforms go thro... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| C.5.2 | Are information security personnel responsible for the design of infor... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| C.5.3 | Are information security personnel responsible for the review of infor... | Yes | Security policies are reviewed... | 3 | 2.4 | 0 | 2.4 | 6 |
| C.5.4 | Do information security personnel review the effectiveness of informat... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| C.5.6 | Does senior management ensure all personnel are provided with a confid... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| C.6 | Does the organization's senior management demonstrate leadership and c... | Yes | Yes, discussed and agreed upon... | 3 | 2.4 | 0 | 2.4 | 6 |
| C.6.3 | Does the organization's board of directors or ownership ensure informa... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| C.6.6 | Does the organization have a plan to quickly correct nonconformities, ... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| C.11 | Is there an approved, documented process for exchanging cybersecurity ... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| C.12 | Is there a documented process that requires cybersecurity information-... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |

## D. Asset and Info Management

***Domain Baselines - Criticality: High | Impact: 4 | Likelihood: 2***

**Domain Risk: 8**

Evidence: -

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| D.1 | Is there a management-approved asset management program that is commun... | Yes | Yes, Gaspar Labs has a policy ... | 4 | 2.4 | 0 | 2.4 | 8 |
| D.1.1 | Does the organization implement and manage a Configuration Management ... | Yes | Gaspar Labs does not leverage ... | 4 | 2.4 | 0 | 2.4 | 8 |
| D.2 | Is there an acceptable use policy for information and associated asset... | Yes | Yes, all internal Gaspar Labs ... | 4 | 2.4 | 0 | 2.4 | 8 |
| D.2.1 | Are constituents made aware of and held accountable to the Acceptable ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| D.2.2 | Is there a policy or procedure for information handling consistent wit... | Yes | Gaspar Labs has defined the fo... | 4 | 2.4 | 0 | 2.4 | 8 |
| D.2.3 | Does the policy or procedure for information handling include access c... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| D.2.4 | Does the policy or procedure for information handling include encrypti... | Yes | All customer data is encrypted... | 4 | 2.4 | 0 | 2.4 | 8 |
| D.2.5 | Does the policy or procedure for information handling include storage ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| D.2.6 | Does the policy or procedure for information handling include electron... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| D.2.7 | Does the policy or procedure for information handling include removabl... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| D.2.8 | Does the policy or procedure for information handling ensure informati... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| D.3 | Is there a records retention policy and retention schedule covering pa... | Yes | Personal data shall only be re... | 4 | 2.4 | 0 | 2.4 | 8 |
| D.3.1 | Is there a data retention/destruction requirement that includes inform... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| D.3.2 | Is scoped data included in a regular data retention review? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| D.3.3 | Is all media containing scoped data disposed of securely? | Yes | Media is destroyed in accordan... | 4 | 2.4 | 0 | 2.4 | 8 |
| D.3.4 | Is scoped data sent or received electronically? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| D.3.5 | Are policies, procedures, and controls for transferring information en... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| D.3.6 | Is scoped data sent or received electronically encrypted in transit wh... | Yes | Encrypted in transit with TLS ... | 4 | 2.4 | 0 | 2.4 | 8 |
| D.3.7 | Does scoped data sent or received electronically include encryption of... | N/A | Customer data is not transmitt... | 4 | 2.4 | 0 | 2.4 | 8 |
| D.3.8 | Does scoped data sent or received electronically include protection ag... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| D.3.9 | Does scoped data sent or received electronically include content filte... | N/A | Customer data is not transmitt... | 4 | 2.4 | 0 | 2.4 | 8 |
| D.3.11 | Is regulated or confidential scoped data stored in a database? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| D.3.11.1 | Does regulated or confidential scoped data stored in a database includ... | Yes | With Azure TDE, AES-256. | 4 | 2.4 | 0 | 2.4 | 8 |
| D.3.12 | Is regulated or confidential scoped data stored in files? | No | Customer data is hosted in clo... | 4 | 2.4 | 0 | 2.4 | 8 |
| D.3.12.1 | Does regulated or confidential scoped data stored in files include fil... | N/A | - | 4 | 2.4 | 0 | 2.4 | 8 |
| D.4 | Is Information classified according to legal or regulatory requirement... | Yes | In accordance with our Asset M... | 4 | 2.4 | 0 | 2.4 | 8 |
| D.5 | Does the organization assign asset ownership to a department, team or ... | Yes | With Azure TDE, AES-256. | 4 | 2.4 | 0 | 2.4 | 8 |
| D.5.1 | Are owners responsible to approve and periodically review access to In... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| D.6 | Is scoped data sent or received via physical media? | No | Customer data is hosted in clo... | 4 | 2.4 | 0 | 2.4 | 8 |
| D.6.1 | Do transport containers protect against physical damage? | N/A | - | 4 | 2.4 | 0 | 2.4 | 8 |
| D.6.2 | Are all the following used when transporting scoped data: chain of cus... | N/A | - | 4 | 2.4 | 0 | 2.4 | 8 |
| D.7 | Has your company implemented a data loss prevention (DLP) security sol... | Yes | Yes, Gaspar Labs utilizes data... | 4 | 2.4 | 0 | 2.4 | 8 |
| D.7.2 | Does the DLP security solution program include a handling process if d... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| D.7.3 | Does the DLP security solution program include a review of the DLP rul... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| D.7.4 | Is all organization email scanned by a DLP security solution? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| D.7.5 | Is all organization outbound web traffic scanned by a DLP security sol... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| D.7.6 | Is the DLP system configured to block unauthorized traffic? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| D.8 | Do scans performed on incoming and outgoing email include phishing pre... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| D.9 | Are scoped systems or data stored or transferred in cloud-based public... | No | Gaspar Labs does not have acce... | 4 | 2.4 | 0 | 2.4 | 8 |
| D.9.1 | Are organization-approved, cloud-based public file sharing solution(s)... | N/A | Customer data is hosted in clo... | 4 | 2.4 | 0 | 2.4 | 8 |
| D.10 | Are encryption keys managed and maintained for scoped data? | Yes | Encryption keys managed by Mic... | 4 | 2.4 | 0 | 2.4 | 8 |
| D.10.1 | Are encryption keys generated in a manner consistent with key manageme... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| D.10.2 | Are encryption keys encrypted at rest and when transmitted? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| D.10.3 | Is there segregation of duties between personnel responsible for key m... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| D.10.4 | Is there an option for clients to manage their own encryption keys? | Yes | Customer managed keys are avai... | 4 | 2.4 | 0 | 2.4 | 8 |
| D.10.5 | Is Asymmetric encryption key length at a minimum of 2048 bits? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| D.11 | Is maintenance and repair of organizational assets performed and logge... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| D.12 | Can clients specify where their data is stored (logically and physical... | Yes | Yes, Gaspar Labs supports a cl... | 4 | 2.4 | 0 | 2.4 | 8 |
| D.13 | Is data segmentation and separation capability between clients provide... | Yes | Yes, each customer is segregat... | 4 | 2.4 | 0 | 2.4 | 8 |
| D.13.1 | Does data segmentation and separation include database segmentation i.... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| D.14 | In the event of a subpoena or forensics incident, is specific data abl... | Yes | Yes, Gaspar Labs is able to pe... | 4 | 2.4 | 0 | 2.4 | 8 |
| D.15 | Does your organization have a Data Protection Officer? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |

## E. Human Resources Security

*Domain Baselines - Criticality: High | Impact: 4 | Likelihood: 2*

**Domain Risk: 8**

Evidence: -

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| E.1 | Are Human Resources policies and procedures approved by management, co... | Yes | Yes, Gaspar Labs has a policy ... | 4 | 2.4 | 0 | 2.4 | 8 |
| E.1.1 | Are background checks performed pre-employment, and conducted periodic... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| E.1.2 | Do Human Resources policies of the organization include constituent ba... | Yes | Yes, all potential Gaspar Labs... | 4 | 2.4 | 0 | 2.4 | 8 |
| E.1.3 | Are constituents required to sign employment agreements? | Yes | All Gaspar Labs employees must... | 4 | 2.4 | 0 | 2.4 | 8 |
| E.1.3.1 | Do employment agreements for constituents include acknowledgement of A... | Yes | Yes, all Gaspar Labs employee... | 4 | 2.4 | 0 | 2.4 | 8 |
| E.1.3.2 | Do employment agreements for constituents include acknowledgement of C... | Yes | Yes, all Gaspar Labs employee... | 4 | 2.4 | 0 | 2.4 | 8 |
| E.1.3.3 | Do employment agreements for constituents include acknowledgement of C... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| E.1.4 | Does senior management require information security personnel to parti... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| E.1.5 | Does the organization have an implemented human resources security pro... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| E.1.6 | Are constituents and new hires required to attend security awareness t... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| E.1.7 | Does the Human Resources security policy include a disciplinary proces... | Yes | Gaspar Labs maintains discipli... | 4 | 2.4 | 0 | 2.4 | 8 |
| E.1.7.1 | Does the disciplinary process include notification to designated perso... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| E.1.8 | Does the Human Resources security policy include constituent accountab... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| E.2 | Does the Human Resources security policy include a process to remove p... | Yes | Access rights and permissions ... | 4 | 2.4 | 0 | 2.4 | 8 |
| E.2.1 | Are exit interviews conducted for terminated constituents that include... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| E.3 | Does the organization have an employee performance process that is doc... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |

## F. Physical and Environmental

*Domain Baselines - Criticality: High | Impact: 4 | Likelihood: 2*

**Domain Risk: 8**

Evidence: -

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| F.1 | Has management approved a physical security program that is communicat... | Yes | Yes, Gaspar Labs has a policy ... | 4 | 2.4 | 0 | 2.4 | 8 |
| F.1.1 | Does the physical security program include a clean desk policy? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| F.1.2 | Are there physical security controls for all secured facilities (e.g.,... | Yes | For Gaspar Labs offices and Mi... | 4 | 2.4 | 0 | 2.4 | 8 |
| F.1.2.2 | Do the physical security controls include electronic-controlled access... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| F.1.3 | Does the organization have a policy or procedure for defining security... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| F.1.4 | Do the physical security controls include a perimeter physical barrier... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| F.1.5 | Do the physical security controls include entry and exit doors alarmed... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| F.1.6 | Do the physical security controls include a mechanism to prevent tailg... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| F.1.7 | Are there physical access authorization controls that include lists of... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| F.1.8 | Do physical access controls include collection of access equipment (e.... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| F.1.9 | Do physical access controls include segregation of duties for issuing ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| F.1.10 | If visitors are permitted in the facility, are they required to sign i... | Yes | In Gaspar Labs offices, after ... | 4 | 2.4 | 0 | 2.4 | 8 |
| F.1.11 | Are visitors required to wear a badge distinguishing them from employe... | Yes | Gaspar Labs office visitors ar... | 4 | 2.4 | 0 | 2.4 | 8 |
| F.1.12 | Are visitor logs maintained for at least 90 days? | Yes | Gaspar Labs maintains visitor ... | 4 | 2.4 | 0 | 2.4 | 8 |
| F.2 | Is there a physical and environmental hazards assessment conducted pri... | Yes | Managed by Microsoft Azure for... | 4 | 2.4 | 0 | 2.4 | 8 |
| F.2.1 | Has the organization properly identified, monitored, mitigated, and im... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| F.2.3 | Is signage required to identify environmental controls within the data... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| F.2.4 | Do environmental controls include water damage protection measures (e.... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| F.2.5 | Do environmental controls include HVAC and humidity controls? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| F.2.6 | Do environmental controls include heat and smoke detectors and fire su... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| F.3 | Is there a loading dock at the facility? | Yes | At Microsoft Azure data center... | 4 | 2.4 | 0 | 2.4 | 8 |
| F.4 | Is there a battery/UPS (Uninterruptible Power Supply) room in offices ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| F.5 | Is there a generator or generator area in offices and/or facility? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| F.6 | Is there a media library to store scoped data? | N/A | Gaspar Labs does not have acce... | 4 | 2.4 | 0 | 2.4 | 8 |
| F.7 | Is there a telecom equipment room? | Yes | In Gaspar Labs offices and Azu... | 4 | 2.4 | 0 | 2.4 | 8 |
| F.8 | Are devices located in a locked server cabinet within the data center? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| F.8.1 | Do server cabinets include restricted access and are logs kept of all ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| F.9 | Do the scoped systems and data reside in a data center? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| F.9.1 | Do other tenants use the data center? | Yes | Microsoft Azure has many clien... | 4 | 2.4 | 0 | 2.4 | 8 |
| F.9.2 | Are locking screensavers on unattended system displays or locks on con... | Yes | Managed by Microsoft Azure. | 4 | 2.4 | 0 | 2.4 | 8 |
| F.9.3 | Does the organization have maintenance support contracts for critical ... | Yes | Managed by Microsoft Azure. | 4 | 2.4 | 0 | 2.4 | 8 |
| F.9.4 | Are tests conducted for any building systems? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| F.9.4.1 | Are UPS systems tested at least annually? | Yes | Managed by Microsoft Azure. | 4 | 2.4 | 0 | 2.4 | 8 |
| F.9.4.2 | Are all security alarm systems tested at least annually? | Yes | Managed by Microsoft Azure. | 4 | 2.4 | 0 | 2.4 | 8 |
| F.9.4.3 | Are all fire alarms tested at least annually? | Yes | Managed by Microsoft Azure. | 4 | 2.4 | 0 | 2.4 | 8 |
| F.9.4.4 | Are all fire suppression systems tested at least annually? | Yes | Managed by Microsoft Azure. | 4 | 2.4 | 0 | 2.4 | 8 |
| F.9.4.5 | Are all generators tested monthly? | Yes | Managed by Microsoft Azure. | 4 | 2.4 | 0 | 2.4 | 8 |

## G. IT Operations Management

***Domain Baselines - Criticality: High | Impact: 4 | Likelihood: 2***

**Domain Risk: 8**

Evidence: -

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| G.1 | Are the organization's Information Technology Operations policies and ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| G.1.1 | Do all IT personnel (e.g., centralized, decentralized, shadow IT) util... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| G.1.2 | Does the organization have a formalized Information Technology (IT) st... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| G.1.4 | Are IT Governance roles and responsibilities for oversight of the use ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| G.1.5 | Are there standard templates utilized by the organization that cover h... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| G.2 | Is there an operational Change Management/Change Control policy or pro... | Yes | Yes, Gaspar Labs has a policy ... | 4 | 2.4 | 0 | 2.4 | 8 |

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| G.2.1 | Does the operational Change Management/Change Control Policy or progra... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| G.2.2 | Does the operational Change Management/Change Control policy or progra... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| G.2.3 | Does the operational Change Management/Change Control policy or progra... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| G.2.4 | Does the operational Change Management/Change Control policy or progra... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| G.3 | Are information security requirements specified and implemented when n... | Yes | Yes, Gaspar Labs has a policy ... | 4 | 2.4 | 0 | 2.4 | 8 |
| G.3.1 | Are new, upgraded, or enhanced systems required to include a determina... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| G.3.2 | Are information security specifications for new, upgraded, or enhanced... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| G.3.3 | Are business continuity requirements considered for new, upgraded, or ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| G.3.4 | Does the organization maintain a maintenance policy and procedure for ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| G.3.5 | Is testing for validation of all implemented controls required for new... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| G.4 | Does the organization have a problem management lifecycle process and ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |

## H. Access Control

***Domain Baselines - Criticality: High | Impact: 4 | Likelihood: 2***

**Domain Risk: 8**

Evidence: -

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| H.1 | Has management approved an access control policy, communicated it to c... | Yes | Yes, Gaspar Labs has a policy ... | 4 | 2.4 | 0 | 2.4 | 8 |
| H.1.1 | Are access control procedures reviewed periodically to keep up with ch... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.1.2 | Are constituents able to access scoped data? | Yes | Access to production environme... | 4 | 2.4 | 0 | 2.4 | 8 |
| H.1.2.1 | Is there a process for identifying, maintaining, and reviewing access,... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.1.2.2 | Does the organization maintain and periodically review records of user... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.1.3 | Are unique IDs required for authentication to applications, operating ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.1.3.1 | Are user IDs that identify roles or access levels, or contain personal... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.1.4 | Is access to applications, operating systems, databases, and network d... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.1.5 | Is there a process to request and receive approval for access to syste... | Yes | Yes, Gaspar Labs has a policy ... | 4 | 2.4 | 0 | 2.4 | 8 |
| H.1.5.1 | Is there segregation of duties for granting access and approving acces... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.1.6 | Are requests for granting access documented, retained and retrievable ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.1.7 | Are privileged user access rights restricted to key roles (i.e., const... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.1.8 | Does the organization have a policy, procedure, or mechanism to ensure... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.1.9 | Are user access rights reviewed at least annually? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.1.10 | Does the organization's process for assigning or revoking physical or ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.1.11 | Does the service provider conduct user and privileged access reviews f... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.1.12 | Are inactive constituent user IDs disabled and deleted after defined p... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.1.13 | Are clients allowed to manage access to their own systems and data? | Yes | Gaspar Labs clients can access... | 4 | 2.4 | 0 | 2.4 | 8 |

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| H.1.14 | Is a standards-based federated ID capability available to clients e.g.... | Yes | SSO supported through SAML 2.0... | 4 | 2.4 | 0 | 2.4 | 8 |
| H.1.15 | Are clients able to receive a list of personnel that will have access ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.1.16 | Is access to systems that store or process scoped data limited by time... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.1.17 | Does the organization have a policy restricting the reuse of user IDs ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.1.18 | Is there an administrative process to address lost, compromised, or da... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.1.19 | Is there a process in the access control system that allows for the re... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.1.21 | Have measures been taken to ensure that client-specific data is not ac... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.2 | Has management approved, communicated, and enforced a password policy ... | Yes | Passwords for internal Gaspar ... | 4 | 2.4 | 0 | 2.4 | 8 |
| H.2.1 | Does the password policy require keeping passwords confidential? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.2.2 | Does the password policy apply to all servers, network devices, web/fi... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.2.3 | Does the password policy mandate periodic password changes, prohibit p... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.2.4 | Does the password policy require passwords to be encrypted or hashed i... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.2.5 | Does the password policy require passwords be masked when entered and ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.2.6 | Does the password policy require system configuration to lock an accou... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.2.7 | Does the password policy require password expiration within 90 days or... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.2.8 | Does the password policy define specific length and complexity require... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.2.9 | Does the password policy define requirements for provisioning and rese... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.2.10 | Is password reset authority restricted to authorized persons and/or an... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.2.11 | Are user IDs and passwords communicated/distributed via separate media... | Yes | For the initial password for G... | 4 | 2.4 | 0 | 2.4 | 8 |
| H.3 | Is Multi-Factor Authentication (MFA) utilized? | Yes | MFA is enabled for internal Ga... | 4 | 2.4 | 0 | 2.4 | 8 |
| H.3.1 | Is Multi-Factor Authentication required for Privileged System Access? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.3.2 | Is Multi-Factor Authentication required for scoped systems and data ac... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.3.3 | Is Multi-Factor Authentication available for client accounts? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.4 | Is there an internet-accessible self-service portal available that all... | Yes | In the Gaspar Labs software pl... | 4 | 2.4 | 0 | 2.4 | 8 |
| H.5 | Are documented log-on banner requirements maintained? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.6 | Does the organization proactively govern account management of individ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.7 | Does the organization have a process for end users to acknowledge and ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| H.13 | Are identity assertions protected, conveyed, and verified before acces... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |

## I. Application Management

***Domain Baselines - Criticality: High | Impact: 4 | Likelihood: 3***

**Domain Risk: 12**

Evidence: -

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| I.1 | Are applications used to transmit, process, or store scoped data? | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.1.1 | Are the development, testing, and staging environments kept separate f... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| I.1.1.1 | Are development, test, and staging environments separated from the pro... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.1.2 | Is there an individual or group responsible for Application Security? | Yes | Gaspar Labs has a Application ... | 4 | 2.5 | 0 | 2.5 | 12 |
| I.1.2.1 | Do application security experts work with developers for every applica... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.1.3 | Is there an established IT Architecture Plan that defines Secure Archi... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.1.4 | Are outside development resources utilized? | No | - | 4 | 3.0 | 0 | 3.0 | 12 |
| I.1.5 | Is scoped data used in the test, development, or QA environments? | No | - | 4 | 3.0 | 0 | 3.0 | 12 |
| I.1.5.1 | Is authorization required when production data is copied to the test e... | N/A | - | 4 | 3.0 | 0 | 3.0 | 12 |
| I.1.5.2 | Is test data destroyed following the testing phase? | N/A | - | 4 | 3.0 | 0 | 3.0 | 12 |
| I.1.6 | Is there formal training for developers that includes security and pri... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.1.7 | Do changes to applications or application code go through a risk asses... | Yes | Yes, Gaspar Labs has an SDLC p... | 4 | 2.5 | 0 | 2.5 | 12 |
| I.1.7.1 | Is a security architecture risk analysis performed when new applicatio... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.1.8 | Are the risks from internal and external sources clearly understood ba... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.1.9 | Are system, vendor, or service accounts disabled for normal operations... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.1.10 | Are web applications configured to follow best practices or security g... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.1.10.1 | Does the organization have a policy or procedure to control access to ... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.1.11 | Do IT support personnel have access to application source libraries? | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.1.12 | Is all access to application source libraries logged? | Yes | Yes, access to application sou... | 4 | 2.5 | 0 | 2.5 | 12 |
| I.1.12.1 | Are audit logs maintained and reviewed for all application source libr... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.1.13 | Are developers permitted to access production environments, including ... | No | No, customer data never leaves... | 4 | 3.0 | 0 | 3.0 | 12 |
| I.2 | Is application development performed? | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.2.1 | Is there a secure software development lifecycle policy that has been ... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.2.2 | Is there a formal Software Development Life Cycle (SDLC) process? | Yes | Yes, Gaspar Labs has an SDLC p... | 4 | 2.5 | 0 | 2.5 | 12 |
| I.2.3 | Is security testing conducted on applications before production? | Yes | Defined in our SDLC policy. | 4 | 2.5 | 0 | 2.5 | 12 |
| I.2.3.1 | Do pre-production application security reviews include testing procedu... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.2.4 | Is there a documented application change management/change control pro... | Yes | Yes, Gaspar Labs has a policy ... | 4 | 2.5 | 0 | 2.5 | 12 |
| I.2.4.1 | Does the application Change Management/Change Control process include ... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.2.4.2 | Does the application Change Management/Change Control process include ... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.2.4.3 | Does the application Change Management/Change Control process include ... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.2.4.4 | Does the change management process include stakeholder communication a... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.2.4.5 | Does the application change management/change control process include ... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.2.4.6 | Does the application change management/change control process include ... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.2.4.7 | Does the application change management/change control process include ... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.2.5 | Is external code in application documentation identified, reviewed for... | Yes | All OSS components are evaluat... | 4 | 2.5 | 0 | 2.5 | 12 |
| I.2.6 | Is open-source software or libraries used to transmit, process, or sto... | Yes | Yes, Gaspar Labs uses open-sou... | 4 | 2.5 | 0 | 2.5 | 12 |
| I.2.6.1 | Are information security reviews conducted and approved for the use or... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| I.2.7 | Is a Secure Code Review performed regularly? | Yes | Yes, Gaspar Labs conducts stat... | 4 | 2.5 | 0 | 2.5 | 12 |
| I.2.7.1 | Do Secure Code Reviews include regular analysis of vulnerability to re... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.3 | Is a web site or web application supported, hosted, or maintained that... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.3.1 | Are security configuration standards documented for web server softwar... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.3.2 | Is an Application Programming Interface (API) available to clients? | Yes | Gaspar Labs has published APIs... | 4 | 2.5 | 0 | 2.5 | 12 |
| I.3.2.1 | Is there a formal security program established to include API security... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.3.2.2 | Is scoped data encrypted in transit within the API for both request an... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.3.2.3 | Are APIs tested for security weaknesses? | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.3.2.4 | Can a client manage access to the APIs? | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.3.3 | Does the organization have logical or physical segregation between web... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.3.4 | Are web server software security configuration standards reviewed and/... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.3.5 | Is HTTPS enabled for all web pages? | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.3.6 | Are all unnecessary/unused services in web server software uninstalled... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.3.7 | Are sample applications and scripts removed from web servers? | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.3.8 | Are all web server software files maintained separate from the Operati... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.3.9 | Are available high-risk web server software security patches applied a... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.3.9.1 | Are all web server patches, service packs, and hot fixes tested, docum... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.3.9.2 | Are web server software patch successes and failures logged? | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.3.10 | Are third party alert services used to keep up to date with the latest... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.3.11 | Are web server software versions that no longer have security patches ... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.3.12 | Are web server software configuration options restricted to authorized... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| I.3.13 | Are compilers, editors, or other development tools present in producti... | No | - | 4 | 3.0 | 0 | 3.0 | 12 |
| I.4 | Are mobile applications that access scoped systems and data developed? | No | - | 4 | 3.0 | 0 | 3.0 | 12 |
| I.4.1 | Are any actions performed by the mobile application to access, process... | N/A | - | 4 | 3.0 | 0 | 3.0 | 12 |

## J. Cybersecurity Incident Mgmt

***Domain Baselines - Criticality: High | Impact: 4 | Likelihood: 2***

**Domain Risk: 8**

Evidence: -

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| J.1 | Has management approved and communicated a Cybersecurity Incident Mana... | Yes | Yes, Gaspar Labs has a policy ... | 4 | 2.4 | 0 | 2.4 | 8 |
| J.1.1 | Has the scope of the Incident Management Program been clearly defined? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| J.4 | Does the organization have a documented Incident Response Plan that ou... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| J.4.1 | Have the defined stakeholders and organizations received the Incident ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| J.4.2 | Does the Incident Response Plan include procedures for evidence collec... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| J.4.3.4 | Are there any specific notification requirements for customers/clients... | Yes | Any specific notification requ... | 4 | 2.4 | 0 | 2.4 | 8 |
| J.4.4 | Is there a specific methodology to regularly review the Incident Respo... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| J.4.5 | Does the Incident Response Plan require identification and mitigation ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| J.4.6 | Does the Incident Response Plan include reporting incidents interdepar... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| J.5 | Is there a specific methodology to regularly review events on scoped s... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| J.5.1 | Does regular security monitoring include alerts for malware infections... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| J.5.2 | Is there an automated system to review and correlate log and/or behavi... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| J.5.3 | Is system and data security monitored 24x7x365, including hosted envir... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| J.5.4 | Does regular security monitoring include daily security alerts for sco... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| J.5.5 | Does regular security monitoring include all changes to user access ri... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| J.5.6 | Does regular security monitoring include tracking all changes to privi... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| J.5.7 | Does regular security monitoring include Network IDS events? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| J.5.8 | Does regular security monitoring include behavioral activity indicatin... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| J.5.9 | Does regular security monitoring include network device security event... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| J.5.10 | Does regular security monitoring include server security events? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| J.5.11 | Does regular security monitoring include Hypervisor security events? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| J.5.12 | Does regular security monitoring include application, Web Server, and ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| J.6 | Is a Cybersecurity Incident/Event Response team available 24x7x365? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| J.7 | Does documentation exist defining which personnel are authorized to sp... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| J.8 | Is there a staffed form of communications (e.g., e-mail, web form, pho... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| J.9 | Is 24x7x365 security event monitoring of the hosting environment perfo... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| J.11 | Has the organization outsourced its incident reporting responsibilitie... | No | - | 4 | 2.4 | 0 | 2.4 | 8 |
| J.13 | Are incidents promptly categorized and prioritized to respond to those... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| J.14 | Are the actions conducted during an incident investigation formally do... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| J.16 | If the organization is a top-level domain (TLD) registry or domain reg... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |

## K. Operational Resilience

***Domain Baselines - Criticality: High | Impact: 4 | Likelihood: 2***

**Domain Risk: 8**

Evidence: -

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| K.1 | Has the organization established a Business Resilience Policy, designa... | Yes | Yes, Gaspar Labs has a policy ... | 4 | 2.4 | 0 | 2.4 | 8 |
| K.1.1 | Do the products and/or services specified in the scope of this assessm... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.1.2 | Does the Business Resilience Program include an individual program own... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.1.3 | Have appropriate actions been taken to ensure that constituents workin... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.1.4 | Does the Business Resilience Program include a formal annual (or more ... | Yes | Gaspar Labs's BCP/DR policy is... | 4 | 2.4 | 0 | 2.4 | 8 |
| K.1.4.1 | Does the Business Resilience Program's annual review cover resource ad... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| K.1.4.2 | Does the annual Business Resilience Program review cover critical supp... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.1.5 | Is there documentation available for the Business Resilience Program, ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.2 | Is there a formal, documented information technology disaster recovery... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.2.1 | Does the disaster recovery exercise and testing program have a designa... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.2.2 | Does disaster recovery testing include cyber, IT, and privacy resource... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.2.3 | Have measurable recovery objectives been established and are test resu... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.2.4 | Is there an annual schedule of planned disaster recovery exercises and... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.2.5 | Is notification and recovery controls for critical service providers i... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.3 | Are there any dependencies on critical third party service providers? | Yes | Microsoft Azure, our cloud-hos... | 4 | 2.4 | 0 | 2.4 | 8 |
| K.3.1 | Are there documented agreements and processes for immediate notificati... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.3.2 | Are all suppliers of critical hardware, network services and facility ... | No | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.3.3 | Have the notification and escalation protocols for key service provide... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.3.4 | Have planned responses to business disruptions been coordinated with c... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.3.5 | When business resilience procedures have been modified that affect key... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.3.6 | Are third parties required to perform, at a minimum, an annual functio... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.3.7 | Are test results and remediation action plans provided by critical ser... | Yes | Gaspar Labs contractually requ... | 4 | 2.4 | 0 | 2.4 | 8 |
| K.3.8 | Are specific availability or service level requirements defined for th... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.4 | Is there a pandemic/infectious disease outbreak plan? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.4.1 | Does the pandemic plan include preventive measures, documented strateg... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.5 | Is scoped data backed up and stored offsite? | Yes | Customer data is backed up and... | 4 | 2.4 | 0 | 2.4 | 8 |
| K.5.1 | Is there a policy or process for the backup of production data? | Yes | Backups for cloud-hosted imple... | 4 | 2.4 | 0 | 2.4 | 8 |
| K.5.2 | Are backup integrity and related restoration procedures tested at leas... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.5.3 | Are backup and replication errors reviewed and resolved as required? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.5.4 | Are offline data backups protected from destructive malware or other t... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.6 | Is there a formal process focused on identifying and addressing risks ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.6.1 | Does an Operational risk assessment consider natural, technological, a... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.7 | Have formal procedures for business continuity been developed and docu... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.7.1 | Does the organization have a procedure to restore the security of info... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.9 | Is there a policy or procedure in place within the organization to ens... | Yes | Gaspar Labs has a documented B... | 4 | 2.4 | 0 | 2.4 | 8 |
| K.9.1 | Does the organization have a policy or procedure in place to guarantee... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.9.2 | Do formal business continuity procedures include specific actions to b... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.9.3 | Do the formal business continuity procedures include manual steps for ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.9.4 | Do formal business continuity procedures include the continuity of inf... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.9.5 | Do formal business continuity procedures include the continuity of IT ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.10 | Has senior management assigned the responsibility for overall manageme... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| K.10.1 | Do response and recovery activities include conditions for activating ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.10.2 | Do response and recovery activities include mechanisms to communicate ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.10.3 | Do response and recovery activities include notification and escalatio... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.11 | Is there a data retention policy or process with a retention schedule ... | Yes | Yes, customer data is retained... | 4 | 2.4 | 0 | 2.4 | 8 |
| K.11.1 | Does the data retention policy define retention history parameters bas... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.11.2 | Does all scoped data fully adhere to the data retention policy? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.12 | Is there a plan for managing a data recovery effort in the aftermath o... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.13 | Has a business impact analysis been conducted? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.13.1 | Is the business impact analysis validated and/or refreshed at least an... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.16 | Is there a periodic (at least annual) review of the business resilienc... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.17 | Are documented disaster recovery procedures regularly reviewed and add... | Yes | Yes, Gaspar Labs has a policy ... | 4 | 2.4 | 0 | 2.4 | 8 |
| K.18 | Is there a backup procedure in place for the organization's informatio... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.18.1 | Does the organization have a procedure for backing up their informatio... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.20 | Does the disaster recovery documentation cover everything, including a... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.21 | Does business continuity testing cover scenarios such as critical pers... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.22 | Are there established business resilience testing exercise scenarios a... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.23 | Is there sufficient redundancy capacity to ensure services are not imp... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.24 | Is there sufficient volume or disk partitioning to prevent inadvertent... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.26 | Is software, configuration settings, and related documentation kept in... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.30 | Is there a resiliency strategy that includes a multi-vendor strategy t... | No | - | 4 | 2.4 | 0 | 2.4 | 8 |
| K.31 | Does the organization have a Threat-Led Penetration Test (TPLT) progra... | Yes | Gaspar Labs uses Protiviti to ... | 4 | 2.4 | 0 | 2.4 | 8 |
| K.36 | Are comprehensive exit plans for ICT services, including appropriate c... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |

## L. Compliance and Ops Risk

***Domain Baselines - Criticality: Medium | Impact: 3 | Likelihood: 2***

**Domain Risk: 6**

Evidence: -

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| L.1 | Are there policies and procedures to ensure compliance with applicable... | Yes | Yes, Gaspar Labs has a policy ... | 3 | 2.4 | 0 | 2.4 | 6 |
| L.1.1 | Is there a documented process to identify and assess regulatory change... | Yes | Yes, Gaspar Labs has a policy ... | 3 | 2.4 | 0 | 2.4 | 6 |
| L.1.1.1 | Does the regulatory change management process include receiving alerts... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| L.1.2 | Are business licenses, permits, or registrations maintained in all jur... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| L.2 | Is a web site(s) maintained or hosted for the purpose of advertising, ... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| L.2.1 | Are terms of sale, dispute and/or return of goods procedures available... | Yes | Please see our website for mor... | 3 | 2.4 | 0 | 2.4 | 6 |
| L.2.2 | Is there a documented process for receiving and responding to inquirie... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| L.2.3 | Is there a documented process to receive and respond to complaints, in... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| L.2.5 | Are due diligence procedures (e.g., screening of third parties and fou... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| L.2.6 | Are Anti-Bribery and Anti-Corruption violation reporting mechanisms, i... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| L.3 | Are there policies and procedures for addressing antitrust and anti-co... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| L.3.1 | Is training on Anti-Trust and Anti-Competitive Business Practices requ... | Yes | Through Gaspar Labs's Employee... | 3 | 2.4 | 0 | 2.4 | 6 |
| L.4 | Is there a documented internal compliance and ethics program? | Yes | Through the Code of Conduct in... | 3 | 2.4 | 0 | 2.4 | 6 |
| L.4.1 | Has the organization established its standards of conduct concerning i... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| L.4.2 | Is there a whistleblowing policy and/or separate communication channel... | Yes | www.Gaspar Labs.com/trust | 3 | 2.4 | 0 | 2.4 | 6 |
| L.4.3 | Do employees undergo annual training regarding company expectations re... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| L.5 | Are documented policies and procedures maintained to enforce applicabl... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| L.5.1 | Are all systems regularly reviewed for compliance with all cybersecuri... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| L.6 | Are there policies and procedures for detecting and preventing interna... | Yes | For Gaspar Labs's Finance team... | 3 | 2.4 | 0 | 2.4 | 6 |
| L.6.1 | Are there documented and defined monitoring and oversight functions fo... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| L.7 | Are there procedures for managing conflicting regulatory record retent... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| L.8 | Is there an internal audit, risk management, or compliance department,... | Yes | Through our internal GRC team.... | 3 | 2.4 | 0 | 2.4 | 6 |
| L.8.1 | Does the internal audit function have independence from the lines of b... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| L.8.2 | Is there non-audit staff dedicated to compliance and risk responsibili... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| L.9 | Is there a compliance program or set of policies and procedures in pla... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| L.9.1 | Is a sanctions risk assessment performed on all relevant entities with... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| L.9.2 | Does the compliance program include compliance and sanction checks (e.... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| L.10 | Do the services in scope for this assessment include providing any cal... | No | - | 3 | 2.4 | 0 | 2.4 | 6 |
| L.11 | Are marketing, selling, or collections activities conducted directly w... | No | - | 3 | 2.4 | 0 | 2.4 | 6 |
| L.12 | Are outbound collections activities conducted directly with Client's c... | No | - | 3 | 2.4 | 0 | 2.4 | 6 |
| L.13 | Is training on legislative and regulatory requirements provided and up... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| L.14 | Is there a set of policies and procedures that address logging, tracki... | Yes | Gaspar Labs reports security a... | 3 | 2.4 | 0 | 2.4 | 6 |
| L.14.1 | Are regulatory alerts and changes in law that impact products or servi... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |
| L.15 | Is there a set of policies and procedures that address Anti-Money Laun... | No | Gaspar Labs addresses Anti-Mon... | 3 | 2.4 | 0 | 2.4 | 6 |
| L.16 | Is there a documented identify theft prevention program approved by ma... | N/A | Gaspar Labs will provide ident... | 3 | 2.4 | 0 | 2.4 | 6 |
| L.17 | Is there a compliance program or set of policies and procedures that a... | Yes | In terms of classification: US... | 3 | 2.4 | 0 | 2.4 | 6 |
| L.18 | Are any entities involved in the delivery of scoped services licensed ... | No | - | 3 | 2.4 | 0 | 2.4 | 6 |
| L.231 | Are there procedures to identify and rectify non-compliance with regul... | Yes | - | 3 | 2.4 | 0 | 2.4 | 6 |

## M. Endpoint Device Security

*Domain Baselines - Criticality: High | Impact: 4 | Likelihood: 2*

**Domain Risk: 8**

Evidence: -

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| M.1 | Do desktops, laptops, tablets, or smartphones transmit, process, or st... | No | Customer data is not stored or... | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.1 | Does the organization's build and hardening standards criteria deploy ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.2 | Are constituents allowed to utilize mobile devices within the organiza... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.3 | Is there a mobile device management program in place that has been app... | N/A | External networks cannot conne... | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.4 | Can constituents access corporate e-mail using mobile devices? | N/A | Gaspar Labs company devices co... | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.5 | Are non-company managed computing devices used to connect to the compa... | No | - | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.6 | Are any mobile devices with access to scoped data Constituent owned (B... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.7 | Does the organization protect the confidentiality, integrity, availabi... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.8 | Are there end user device security configuration standards? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.9 | Are defined procedures in place to identify and correct systems withou... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.10 | Are mobile devices evaluated as part of the IT Risk Management program... | N/A | Microsoft Azure manages the se... | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.11 | Can constituents access, view, store and connect to scoped data/system... | Yes | Through our WAF, Cloudflare. | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.12 | Is a technical solution in place to enforce mobile device security req... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.13 | Prior to device on-boarding are constituents required to sign a legal ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.14 | Is there a process or procedure for responding to mobile device data c... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.15 | Is there an approved process for IT to offboard mobile devices when a ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.16 | Is the identity management system (directory services) integrated with... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.17 | Are mobile operating system versions that are deemed end of life permi... | No | - | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.18 | Are all unnecessary/unused services uninstalled or disabled for end us... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.19 | Are all available high-risk security patches applied and verified at l... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.20 | Are end user device operating system versions that no longer have patc... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.21 | Are anti-malware software version and engine upgrade deployment failur... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.22 | Are periodic configuration reviews performed at least quarterly and wh... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.23 | Is there a requirement to physically secure end user systems when left... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.24 | Are there controls to protect scoped data stored on portable media or ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.25 | Is security approval required prior to implementing non-standard compu... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.26 | Is security approval required prior to implementing freeware or sharew... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.27 | Is installation of software on company-owned equipment (e.g., workstat... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.28 | Is a Virtual Desktop Infrastructure used for accessing, transmitting, ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| M.1.29 | Does the organization have policies, procedures, or mechanisms in plac... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| M.2 | Does the organization have a policy or procedure to train personnel on... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| M.3 | Does the organization maintain policies and procedures for the access ... | N/A | - | 4 | 2.4 | 0 | 2.4 | 8 |
| M.3.1 | Does the organization use authorized devices for collaboration on sens... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |

## N. Network Security

***Domain Baselines - Criticality: High | Impact: 4 | Likelihood: 2***

**Domain Risk: 8**

Evidence: -

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| N.1 | Does the organization build and maintain a secure network and systems? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.1.1 | Does the organization have processes and mechanisms that are defined a... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.1.2 | Does the organization have a process to configure and maintain network... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.1.2.1 | Does the organization execute all changes to network connections and c... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.2 | Does the organization have a Network Security Program with a defined p... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.2.1 | Are reviews performed to validate compliance with documented network d... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.3 | Is every connection to an external network terminated at a firewall e.... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.3.1 | Are network or security technologies used to establish and enforce sec... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.3.2 | Are all firewall and other network Access Control List (ACL) rules rev... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.3.2.1 | Does the organization have protocols to identify and continuously addr... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.3.3 | Is there a separate network segment or dedicated endpoints for remote ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.3.4 | Do all network segmentation and segregation technologies enforce the p... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.4 | Are all network devices patched with all, available high-risk security... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.4.1 | Does network device patching include testing of patches, service packs... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.5 | Has management approved a policy for remote access to scoped systems a... | Yes | Remote access is through a bas... | 4 | 2.4 | 0 | 2.4 | 8 |
| N.5.1 | Are encrypted communications required for all remote network connectio... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.5.2 | Is remote administration of organizational assets approved, logged, an... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.5.3 | Are Split Tunneling and Bridged Internet Connections while remotely co... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.5.4 | Is multi-factor authentication required for all remote network connect... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.5.5 | Is remote access and communication paths of access monitored? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.7 | Are Network Intrusion Detection/Prevention Systems (NIDS/NIPS) employe... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.7.1 | Are Network Intrusion Detection signatures updated on a periodic basis... | Yes | Automatically updated with new... | 4 | 2.4 | 0 | 2.4 | 8 |
| N.8 | Is there an DMZ environment within the network that transmits, process... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.8.1 | Are DMZ environments divided into isolated DMZ network segments for de... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.9 | Is there a wireless policy or program that has been approved by manage... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.10 | Are the perimeters of each domain clearly defined on separate networks... | Yes | Yes, each domain is clearly de... | 4 | 2.4 | 0 | 2.4 | 8 |

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| N.10.1 | Are the networks segmented into domains based on an evaluation of the ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.10.2 | Does the Wireless Security Policy require wireless connections to be s... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.10.3 | Does the Wireless Security Policy require approved, and vendor support... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.11 | Are there security standards, baseline configurations, patching, acces... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.12 | Are default passwords changed or disabled prior to placing network dev... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.13 | Is there an approval process prior to installing a network device? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.13.1 | Is there a process that requires security approval to allow external n... | N/A | External networks cannot conne... | 4 | 2.4 | 0 | 2.4 | 8 |
| N.13.2 | Is security approval required to connect a device on the company netwo... | N/A | Gaspar Labs company devices co... | 4 | 2.4 | 0 | 2.4 | 8 |
| N.13.3 | Is there a process that requires security approval to allow connection... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.14 | Are all network device administrative interfaces configured to require... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.15 | Are corporate standardized Simple Network Management Protocol (SNMP) C... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.16 | Is there sufficient detail contained in network device logs to support... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| N.17 | Are third party support personnel granted remote network access only u... | Yes | Third party support personnel ... | 4 | 2.4 | 0 | 2.4 | 8 |
| N.18 | Are Baseboard Management Controllers (BMCs) enabled on any servers or ... | N/A | Microsoft Azure manages the se... | 4 | 2.4 | 0 | 2.4 | 8 |
| N.19 | Are mechanisms implemented to achieve resilience requirements in norma... | Yes | Through our WAF, Cloudflare. | 4 | 2.4 | 0 | 2.4 | 8 |

## O. Environ, Social, Gov (ESG)

***Domain Baselines - Criticality: Medium | Impact: 3 | Likelihood: 3***

**Domain Risk: 9**

Evidence: -

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| O.1 | Does the organization have and adhere to an environmental policy that ... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| O.1.1 | Does the organization's environmental policy cover climate change issu... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| O.1.2 | Does the organization incorporate consideration of climate risks into ... | No | - | 3 | 3.5 | 0 | 3.5 | 12 |
| O.1.3 | Does the organization's environmental policy have executive and board-... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| O.1.4 | Does the insurer have a written policy approved by its board that outl... | No | - | 3 | 3.5 | 0 | 3.5 | 12 |
| O.1.5 | Is the organization taking into account the impact of climate-related ... | No | - | 3 | 3.5 | 0 | 3.5 | 12 |
| O.1.6 | Is the organization's environmental policy regularly reviewed and upda... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| O.2 | Does the organization have material discharges to air as a direct resu... | No | - | 3 | 3.5 | 0 | 3.5 | 12 |
| O.3 | Does the organization have processes to ensure that there are no mater... | N/A | - | 3 | 3.5 | 0 | 3.5 | 12 |
| O.4 | Has the organization implemented procedures to ensure the safe use, ha... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| O.5 | Does the organization maintain processes to ensure there are no advers... | No | - | 3 | 3.5 | 0 | 3.5 | 12 |
| O.6 | Are there any financial provisions in the annual accounting statements... | No | - | 3 | 3.5 | 0 | 3.5 | 12 |
| O.7 | Does the organization have documented policies and procedures in place... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| O.8 | Does the organization ensure that sub-contractors are treated fairly a... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| O.9 | Does the organization have a documented policy on Health and Safety? | Yes | As a global company with entit... | 3 | 2.5 | 0 | 2.5 | 9 |
| O.10 | Has the organization established formal community relations programs t... | No | - | 3 | 3.5 | 0 | 3.5 | 12 |
| O.11 | Does the organization have policies to ensure products and services do... | N/A | - | 3 | 3.5 | 0 | 3.5 | 12 |
| O.12 | Does the organization have a formalized Environmental, Social, and Gov... | No | Gaspar Labs does have a formal... | 3 | 3.5 | 0 | 3.5 | 12 |
| O.12.1 | Are the organization's Environmental, Social, and Governance (ESG) pol... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| O.13 | Does the organization have a formal diversity, equity, and inclusion (... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| O.13.1 | Does the organization have a formal commitment or policy to supplier d... | No | - | 3 | 3.5 | 0 | 3.5 | 12 |
| O.13.2 | Does the organization publish an external report on its Environmental,... | No | - | 3 | 3.5 | 0 | 3.5 | 12 |
| O.14 | Does the organization have a documented policy for Ethical Sourcing? | No | This program is in the process... | 3 | 3.5 | 0 | 3.5 | 12 |
| O.14.1 | Does the organization have a responsible purchasing procedure or stand... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| O.14.2 | Does the organization have a defined supplier code of conduct required... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| O.14.3 | Has the organization published a clear statement of its Environmental,... | Yes | Gaspar Labs has implemented a ... | 3 | 2.5 | 0 | 2.5 | 9 |
| O.14.4 | Does the organization evaluate its suppliers based on its Environmenta... | No | - | 3 | 3.5 | 0 | 3.5 | 12 |
| O.14.5 | Does the organization include defined standards in the Procurement and... | No | - | 3 | 3.5 | 0 | 3.5 | 12 |
| O.15 | Has the organization conducted a baseline assessment of its carbon/Gre... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| O.16 | Is the organization compliant with carbon and Greenhouse Gas (GHG) req... | No | No, but this is included in ou... | 3 | 3.5 | 0 | 3.5 | 12 |
| O.17 | Is the organization aware of any past or current soil or groundwater c... | No | - | 3 | 3.5 | 0 | 3.5 | 12 |
| O.18 | Are renewable resources being utilized by the organization? | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| O.19 | Does the organization have any processes to monitor and reduce energy ... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| O.20 | Does the organization assess opportunities to generate its sources of ... | No | - | 3 | 3.5 | 0 | 3.5 | 12 |
| O.21 | Have initiatives been put in place by the organization to monitor and ... | No | - | 3 | 3.5 | 0 | 3.5 | 12 |
| O.22 | Does the organization have processes to avoid generating material quan... | No | - | 3 | 3.5 | 0 | 3.5 | 12 |
| O.23 | Does the organization have and follow procedures for responsible dispo... | N/A | - | 3 | 3.5 | 0 | 3.5 | 12 |
| O.24 | Does the organization have a compliance program and procedures that ad... | No | As a global company with entit... | 3 | 3.5 | 0 | 3.5 | 12 |
| O.25 | Does the organization have a formal and functional grievance mechanism... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| O.26 | Do all employees in the organization meet minimum age standards and re... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| O.27 | Do all employees in the organization meet minimum wage standards and r... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| O.28 | Has the organization created, put into practice, and regularly reviewe... | Yes | As a global company with entit... | 3 | 2.5 | 0 | 2.5 | 9 |
| O.29 | Does the organization provide all employees and contractors with healt... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| O.29.1 | Has the organization documented and implemented formal processes for r... | No | - | 3 | 3.5 | 0 | 3.5 | 12 |
| O.30 | Does the organization have a policy for ensuring the diversity of boar... | No | - | 3 | 3.5 | 0 | 3.5 | 12 |
| O.31 | Is the organization's Board of Directors monitoring Environmental, Soc... | No | - | 3 | 3.5 | 0 | 3.5 | 12 |
| O.32 | Has the organization implemented Environmental, Social, and Governance... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| O.33 | Does the organization have a process to regularly evaluate relevant En... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| O.34 | Does the organization have a functional and certified data protection,... | Yes | Gaspar Labs has implemented te... | 3 | 2.5 | 0 | 2.5 | 9 |
| O.34.1 | Is the organization aware of any breaches in cybersecurity within the ... | No | - | 3 | 3.5 | 0 | 3.5 | 12 |

## P. Privacy

***Domain Baselines - Criticality: High | Impact: 4 | Likelihood: 2***

**Domain Risk: 8**

Evidence: -

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| P.1 | Is there collection, access, processing, disclosure, or retention of a... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.1.1 | Is client scoped data collected, accessed, transmitted, processed, dis... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.1.2 | Is client scoped data collected, accessed, transmitted, processed, dis... | No | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.1.2.1 | Does client scoped data include the disclosure of identifiers to the c... | N/A | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.1.2.2 | Do contracts between parties, including fourth parties, specify the ob... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.1.2.3 | Do contracts between parties, including fourth parties, specify the li... | N/A | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.2 | Does the organization have a policy for preserving privacy and protect... | Yes | Please see our Privacy Notice ... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.2.1 | Is client scoped data collected, accessed, processed, disclosed, or re... | No | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.2.1.1 | Are there policies and procedures for secure disposal of consumer info... | N/A | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.2.2 | Is client scoped data collected, accessed, transmitted, processed, dis... | Yes | For companies that must comply... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.2.2.1 | Are there documented policies and procedures to detect and report unau... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.2.2.2 | Is there a Business Associate Agreement (BAA) contract in place to add... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.2.3 | Is client scoped data collected, accessed, transmitted, processed, or ... | Yes | Yes, Gaspar Labs stores and pr... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.2.3.1 | If client scoped data includes data of residents of any geographical a... | Yes | www.Gaspar Labs.com/privacy-no... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.2.3.2 | Does the contract of the organization require any authorized users tha... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.2.4 | Is client scoped data collected, accessed, transmitted, processed, dis... | Yes | Yes, Gaspar Labs stores and pr... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.2.4.1 | Are there policies and procedures in place that apply specific restric... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.2.4.2 | Are there cross border data flows or international transfers of client... | Yes | As part of our commitment to m... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.2.4.2.1 | Are there documented policies and procedures to address cross border d... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.2.4.3 | Is there a process in place to erase personal data based on privacy ri... | Yes | Customer data is stored encryp... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.2.5 | Is client scoped data collected, transmitted, processed, disclosed, or... | Yes | Yes, Gaspar Labs stores and pr... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.2.5.1 | Does the organization have policies and procedures in place to require... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.2.6 | Is client scoped data collected, accessed, transmitted, processed, or ... | No | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.2.7 | Is client scoped data of minors collected, transmitted, processed, dis... | No | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.2.7.1 | Does the organization maintain an external safe harbor certification f... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| P.2.7.5 | Does the organization maintain policies and procedures that limit the ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.3 | Has the organization developed and maintained a formal privacy program... | Yes | Yes, please see our Privacy No... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.3.1 | Is documentation of the data processing environment, including the rol... | Yes | Gaspar Labs maintans an applic... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.3.1.1 | Is there a formalized approval process to review and update data class... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.3.1.4 | Does the data inventory include the categories of types of individuals... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.3.1.5 | Does the data inventory identify the specific data elements used withi... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.3.2 | Does the privacy program plan describe the structure of dedicated priv... | Yes | Yes, please see our Privacy No... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.3.2.1 | Is the privacy program plan reviewed annually and approved by senior m... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.3.2.2 | Is there a management procedure maintained to address changes to the p... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.3.3 | Has a qualified individual been designated as a Privacy Executive or P... | Yes | Gaspar Labs has a Global DPO, ... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.3.3.1 | Does the organization's board of directors or ownership require manage... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.3.4 | Is there an ongoing process to regularly review and update privacy pol... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.4 | Is there a training and awareness program that addresses data privacy ... | Yes | Yes, all Gaspar Labs employees... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.4.1 | Is privacy awareness training for constituents, including privacy pers... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.4.2 | Is there a mechanism in place to receive requests and address restrict... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.5 | Are there documented policies and procedures that define limits to the... | Yes | Gaspar Labs will only use data... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.5.1 | Is there a documented policy or process to maintain accurate, complete... | Yes | In accordance with our Asset M... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.5.1.1 | Are procedures documented that outline the relevancy of the personal i... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.5.2 | Is personal information collected directly from an individual by the o... | Yes | PII is collected by Gaspar Lab... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.5.2.1 | Are there documented privacy policies and procedures that address choi... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.5.3 | Does the organization obtain personal information directly from the cl... | Yes | PII is inserted into the appli... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.5.3.1 | Are there policies and procedures that address data collection, purpos... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.5.3.2 | Is there a policy and process to limit any secondary use of client sco... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.5.3.3 | Are there policies and processes in place to support the client in res... | Yes | Gaspar Labs will assist in the... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.5.3.3.1 | Does the process enable the individual to access, correct, or delete i... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.5.3.3.2 | Can the individual request an electronic copy of their personal inform... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.5.3.3.3 | Is there a documented process to reasonably authenticate or verify an ... | Yes | Managed through the Gaspar Lab... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.5.4 | Is there an oversight function or compliance management system that ad... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.6 | Does the organization have or maintain internet-facing website(s), mob... | Yes | Yes, Gaspar Labs stores and pr... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.6.1 | Is a web privacy policy or notice provided to the individual at the ti... | Yes | Please see our Privacy Notice ... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.6.1.1 | Do privacy notices include the categories of personal information coll... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.6.1.2 | Is notice provided at or before point of collection regarding the sell... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.6.1.3 | Does the privacy notice include information about the web or digital t... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.6.1.4 | Does the platform, site, and/or application provide a mechanism to add... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| P.7 | Does the organization have policies and procedures for conducting peri... | Yes | Yes, Gaspar Labs conducts PIAs... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.7.1 | Are privacy risks or control gaps identified, prioritized, and include... | Yes | Please see our Privacy Notice ... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.7.1.1 | Does the organization maintain criteria and conditions that trigger co... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.8 | Does the organization have a data governance program and designated bo... | Yes | Gaspar Labs is committed to pr... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.8.1 | Are tests conducted at least annually of the effectiveness of the key ... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.8.2 | Are descriptions of the data protection safeguards available to indivi... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.8.3 | Is there a Third Party Risk Management Program (including ongoing moni... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.8.4 | Is client scoped data aggregated, appended, profiled, or modeled using... | No | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.8.5 | Are there control mechanisms in place to de-identify, mask, anonymize,... | Yes | Customer data is stored encryp... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.8.6 | Do the procedures include opt-in and opt-out requirements for the serv... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.9 | Are there policies and procedures in place to detect and report privac... | Yes | If it becomes aware of a secur... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.9.1 | Is there a process in place to identify and report privacy incidents i... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.10 | Do any other parties (e.g., affiliates, fourth-Nth parties, contractor... | Yes | Gaspar Labs uses sub-processor... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.10.1 | Do agreements with fourth parties who have access to or potential acce... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| P.11 | Is there a data privacy or data protection role accountable for compli... | Yes | Gaspar Labs is committed to pr... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.11.1 | Are there policies and procedures in place to provide individual notic... | Yes | Please refer to our Privacy No... | 4 | 2.4 | 0 | 2.4 | 8 |
| P.12 | If necessary, does the organization have a process to ensure that its ... | No | Gaspar Labs reviews annually o... | 4 | 2.4 | 0 | 2.4 | 8 |

## R. AI Governance

***Domain Baselines - Criticality: Medium | Impact: 3 | Likelihood: 3***

**Domain Risk: 9**

Evidence: -

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| R.1 | Does the organization have a process to inform personnel of legal and ... | Yes | Gaspar Labs is dedicated to bu... | 3 | 2.5 | 0 | 2.5 | 9 |
| R.1.1 | Are AI risk management practices aligned with applicable legal standar... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| R.2 | Do organizational policies, processes, and procedures include the char... | Yes | Gaspar Labs has published an A... | 3 | 2.5 | 0 | 2.5 | 9 |
| R.2.1 | Is the AI Policy aligned to broader data governance policies and pract... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| R.4 | Does the organization monitor and perform a periodic review of the AI ... | Yes | Gaspar Labs has performed a ri... | 3 | 2.5 | 0 | 2.5 | 9 |
| R.4.1 | Does the organization establish policies and procedures for monitoring... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| R.5 | Does the organization establish policies that define the creation and ... | Yes | Gaspar Labs does establish pro... | 3 | 2.5 | 0 | 2.5 | 9 |
| R.5.1 | Does the organization establish policies to define mechanisms for meas... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| R.6 | Does the organization establish an accountability structure so that th... | Yes | Gaspar Labs has defined and co... | 3 | 2.5 | 0 | 2.5 | 9 |
| R.6.1 | Does the organization establish policies and procedures regarding AI a... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| R.7 | Does the organization establish AI policies for personnel addressing o... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| R.7.1 | Does training include organizational AI policies? | Yes | The general consensus is that ... | 3 | 2.5 | 0 | 2.5 | 9 |
| R.7.1.1 | Does the training include trustworthy AI characteristics? | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| R.7.2 | Does the organization establish or identify, and document reliability ... | Yes | Gaspar Labs tracks model metri... | 3 | 2.5 | 0 | 2.5 | 9 |
| R.7.3 | Does the AI Policy establish a frequency of and detail for monitoring,... | Yes | Our current policy is to launc... | 3 | 2.5 | 0 | 2.5 | 9 |
| R.7.4 | Does the AI Policy include testing for incident response plans? | No | Any security incidents follow ... | 3 | 3.5 | 0 | 3.5 | 12 |
| R.7.5 | Is there a process to evaluate AI system purpose in consideration of p... | Yes | We conduct AI risk assessments... | 3 | 2.5 | 0 | 2.5 | 9 |
| R.7.6 | Does the organization establish policies for AI system incident respon... | Yes | Any security incidents follow ... | 3 | 2.5 | 0 | 2.5 | 9 |
| R.8 | Does the organization establish policies that define which models or s... | No | Gaspar Labs does not define po... | 3 | 3.5 | 0 | 3.5 | 12 |
| R.9 | Does the organization establish risk tolerance levels for AI systems a... | Yes | Gaspar Labs sets risk threshol... | 3 | 2.5 | 0 | 2.5 | 9 |
| R.10 | Does the organization establish policies that define the AI risk manag... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| R.11 | Does the organization plan and test human-AI configurations under clos... | Yes | All of Gaspar Labs's AI capabi... | 3 | 2.5 | 0 | 2.5 | 9 |
| R.11.1 | Is connectivity of the AI system or data it will have to external netw... | Yes | All AI capabilities are subjec... | 3 | 2.5 | 0 | 2.5 | 9 |
| R.11.2 | Does the organization have a documented and executable process to iden... | No | While Gaspar Labs has internal... | 3 | 3.5 | 0 | 3.5 | 12 |
| R.12 | Does the organization have mechanisms to regularly communicate and col... | Yes | Feedback is stored in customer... | 3 | 2.5 | 0 | 2.5 | 9 |
| R.12.1 | Does the organization document assumptions made and techniques used in... | Yes | We use free-to-use publicly av... | 3 | 2.5 | 0 | 2.5 | 9 |
| R.12.1.1 | Does the organization document assumptions made and techniques used in... | N/A | Gaspar Labs does not provide A... | 3 | 3.5 | 0 | 3.5 | 12 |
| R.12.1.1.1 | Does the organization identify and document transparent methods (e.g.,... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| R.12.1.1.2 | Does the organization establish and document processes to test and ver... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| R.13 | Does the organization employ personnel to work with domain experts and... | Yes | Our internal privacy team ens... | 3 | 2.5 | 0 | 2.5 | 9 |
| R.14 | Does the organization establish policies and procedures that define an... | No | - | 3 | 3.5 | 0 | 3.5 | 12 |
| R.15 | Does the organization establish policies that require inclusion of ove... | No | - | 3 | 3.5 | 0 | 3.5 | 12 |
| R.16 | Does the organization define and develop training materials for propos... | Yes | Gaspar Labs develops training ... | 3 | 2.5 | 0 | 2.5 | 9 |
| R.18 | Does the organization identify and implement procedures for regularly ... | Yes | All of Gaspar Labs's AI capabi... | 3 | 2.5 | 0 | 2.5 | 9 |
| R.18.1 | Does the organization have a process to identify and declare AI system... | N/A | Gaspar Labs does not provide A... | 3 | 3.5 | 0 | 3.5 | 12 |

## S. Supply Chain Risk Mgmt

***Domain Baselines - Criticality: Medium | Impact: 3 | Likelihood: 3***

**Domain Risk: 9**

Evidence: -

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| S.1 | Does your organization have access control policies for suppliers, dev... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| S.1.1 | Are access control policies stated for all service providers, and do c... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| S.2 | Does the organization ensure proper access control in its systems and ... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| S.3 | Can prime contractors restrict information sharing with sub-tier contr... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| S.4 | Is remote access restricted to employees and contractors during specif... | Yes | Yes, data containers are used ... | 3 | 2.5 | 0 | 2.5 | 9 |
| S.4.1 | Does the organization have clear wireless access control policies for ... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| S.9 | Is access control in place to support authorized supply chain access w... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| S.9.4 | Is there a designated person responsible for creating, documenting, an... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| S.9.5 | Are there procedures and tools in place for recording any detectable i... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| S.17 | Does the organization require primary contractors to implement cross-o... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| S.18 | Does the organization's control assessment plan include controls for m... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| S.22 | Is there a configuration management capability for the organization th... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| S.32 | Is there a documented, approved Cybersecurity Supply Chain Risk Manage... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| S.33 | Has the organization established and put in place a contingency plan f... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| S.34 | Is the organization conducting contingency testing that includes its c... | No | We involve Microsoft Azure in ... | 3 | 3.0 | 0 | 3.0 | 9 |
| S.46 | Is there a procedure in place to ensure that critical (vital per NIST ... | No | Gaspar Labs contractually requ... | 3 | 3.0 | 0 | 3.0 | 9 |
| S.47 | Is it ensured by the organization that the critical suppliers partake ... | No | Gaspar Labs contractually requ... | 3 | 3.0 | 0 | 3.0 | 9 |
| S.48 | Do the organization's supplier agreements contain provisions for track... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| S.51 | Is it ensured by the organization that C-SCRM is incorporated into mai... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| S.57 | Do the organization's media protection policies and procedures cover s... | Yes | Gaspar Labs has an SDLC proces... | 3 | 2.5 | 0 | 2.5 | 9 |
| S.57.1 | Does media storage control encompass C-SCRM activities? | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| S.57.3 | Does the organization incorporate C-SCRM practices and requirements in... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| S.58 | Is the organization ensuring that only authorized individuals who requ... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| S.61 | Does the organization integrate C-SCRM when developing a security plan... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| S.61.1 | Does the organization make sure that contractor organizations are acco... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| S.62 | Is there a process in place within the organization, with the support ... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| S.62.1 | Does the organization have a system in place to ensure effective commu... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| S.80 | Do the security policies and plans clearly define personnel responsibi... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| S.80.1 | Are there procedures or measures to reduce the risk of insider threats... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| S.80.2 | Does the organization confirm that third-party personnel who access it... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| S.80.3 | Does the organization have policies in place to ensure that agreements... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| S.100 | Do the organization's system and communications protection policies an... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| S.101 | Has the organization put in place a defined structure and procedure fo... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |
| S.102 | Is there a reliable system in place to monitor the connections between... | Yes | - | 3 | 2.5 | 0 | 2.5 | 9 |

## T. Threat Management

***Domain Baselines - Criticality: High | Impact: 4 | Likelihood: 2***

**Domain Risk: 8**

Evidence: -

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| T.1 | Is there a centrally managed Vulnerability Management Program and asso... | Yes | Gaspar Labs utilizes daily vul... | 4 | 2.4 | 0 | 2.4 | 8 |
| T.1.1 | Are network Vulnerability Scans performed against internal networks an... | Yes | Yes, Gaspar Labs utilizes dail... | 4 | 2.4 | 0 | 2.4 | 8 |

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| T.1.1.1 | Do internal network vulnerability scans occur periodically? Please def... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| T.1.2 | Are network vulnerability scans performed against internet-facing netw... | Yes | Yes, Gaspar Labs utilizes dail... | 4 | 2.4 | 0 | 2.4 | 8 |
| T.1.2.1 | Do external network vulnerability scans occur periodically? Please def... | Yes | Daily | 4 | 2.4 | 0 | 2.4 | 8 |
| T.1.2.2 | Do external network vulnerability scans occur after a change? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| T.1.3 | Are vulnerabilities documented and tracked to remediation? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| T.1.4 | Are penetration tests performed? | Yes | Gaspar Labs conducts penetrati... | 4 | 2.4 | 0 | 2.4 | 8 |
| T.1.4.1 | Are penetration tests performed periodically? Please define the freque... | Yes | Penetration testing is perform... | 4 | 2.4 | 0 | 2.4 | 8 |
| T.1.4.2 | Do penetration tests procedures include manual in addition to automate... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| T.1.4.3 | Is penetration testing performed on external systems from the Internet... | Yes | Penetration testing is conduct... | 4 | 2.4 | 0 | 2.4 | 8 |
| T.1.4.3.1 | Are web applications included in penetration tests? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| T.1.4.4 | Are penetration test issues documented and tracked to remediation? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| T.1.4.5 | Is penetration testing performed after significant changes? | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| T.1.5 | Are vulnerabilities ranked for importance to the system and vulnerabil... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| T.2 | Does the organization maintain policies, standards, and procedures for... | Yes | Gaspar Labs conducts a risk as... | 4 | 2.4 | 0 | 2.4 | 8 |
| T.2.1 | Does the organization conduct risk assessments to identify and address... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |
| T.3 | Are software updates delivered to clients through automatic downloads ... | Yes | All public-cloud hosted client... | 4 | 2.4 | 0 | 2.4 | 8 |
| T.4 | Are there policies and processes to secure threat and vulnerability as... | Yes | In accordance with access mana... | 4 | 2.4 | 0 | 2.4 | 8 |
| T.4.1 | Is there a documented process in place to protect against and detect a... | Yes | - | 4 | 2.4 | 0 | 2.4 | 8 |

## U. Server Security

***Domain Baselines - Criticality: High | Impact: 4 | Likelihood: 3***

**Domain Risk: 12**

Evidence: -

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| U.1 | Are servers used for transmitting, processing, or storing scoped data? | Yes | Web servers hosted through Mic... | 4 | 2.5 | 0 | 2.5 | 12 |
| U.1.1 | Are server security standards reviewed and/or updated at least annuall... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| U.1.2 | Are all unnecessary/unused services uninstalled or disabled on all ser... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| U.1.3 | Are vendor default passwords removed, disabled, or changed prior to pl... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| U.1.4 | Are all systems and applications patched regularly? | Yes | Yes, Microsoft Azure provides ... | 4 | 2.5 | 0 | 2.5 | 12 |
| U.1.4.1 | Are there any Operating System versions in use within the Scoped Servi... | No | Gaspar Labs does not use end o... | 4 | 3.0 | 0 | 3.0 | 12 |
| U.1.4.2 | Are all available high-risk security patches applied and verified at l... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| U.1.4.3 | Are all server patches, service packs and hot fixes tested prior to in... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| U.1.4.4 | Do patch management processes include evaluation and prioritization of... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| U.1.5 | Are Windows servers used to process, store data or used for scoped ser... | Yes | Yes, Windows servers are used ... | 4 | 2.5 | 0 | 2.5 | 12 |
| U.1.5.1 | Is there an anti-malware policy or program including a means of protec... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| U.1.5.2 | Has the organization deployed antivirus and anti-malware solutions? | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| U.1.6 | Is Unix or Linux used to process, store data or used for scoped servic... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| U.1.6.1 | Are users required to 'su' or 'sudo' into root? | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| U.1.7 | Are AS/400s used to process, store data or used for scoped services? | No | No, AS/400s are not used as pa... | 4 | 3.0 | 0 | 3.0 | 12 |
| U.1.7.1 | Do group profile assignments consider the roles of the constituents, a... | - | - | 4 | 3.0 | 0 | 3.0 | 12 |
| U.1.8 | Are Mainframes used to process, store data or used for scoped services... | No | No, Mainframes are not used as... | 4 | 3.0 | 0 | 3.0 | 12 |
| U.1.8.1 | Is authentication required to access mainframe transactions or databas... | - | - | 4 | 3.0 | 0 | 3.0 | 12 |
| U.1.9 | Are Hypervisors used to manage systems used to transmit, process, or s... | Yes | Hypervisors are managed by Mic... | 4 | 2.5 | 0 | 2.5 | 12 |
| U.1.9.1 | Are all Hypervisors hardened and kept up-to-date with patches? | Yes | Hypervisors are managed by Mic... | 4 | 2.5 | 0 | 2.5 | 12 |
| U.1.9.2 | Are unnecessary/unused Hypervisor services turned off? | Yes | Hypervisors are managed by Mic... | 4 | 2.5 | 0 | 2.5 | 12 |
| U.1.9.3 | Are Hypervisor logs retained for a minimum of one year? | Yes | Hypervisors are managed by Mic... | 4 | 2.5 | 0 | 2.5 | 12 |
| U.1.9.4 | Does the Hypervisor system lock accounts after 3-05 invalid login atte... | Yes | Hypervisors are managed by Mic... | 4 | 2.5 | 0 | 2.5 | 12 |
| U.1.9.5 | Is administrative access restricted to Hypervisor management interface... | Yes | Hypervisors are managed by Mic... | 4 | 2.5 | 0 | 2.5 | 12 |
| U.1.9.6 | Is the host operating system management interface on a separate networ... | Yes | Hypervisors are managed by Mic... | 4 | 2.5 | 0 | 2.5 | 12 |
| U.1.10 | Are all servers configured to log users out after 15 minutes of inacti... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| U.1.11 | Is sufficient detail contained in operating system, database, and appl... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| U.1.11.1 | Are operating system, database, and application events relevant to sup... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| U.1.12 | Are containers used to process or store scoped data e.g., Docker, Kube... | Yes | Yes, data containers are used ... | 4 | 2.5 | 0 | 2.5 | 12 |
| U.1.12.1 | Is there a data container security policy approved by management, comm... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| U.1.12.2 | Are vulnerability scans performed against all containers using tools t... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| U.1.13 | Is an alert generated if removable media (floppy disk, recordable CD, ... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| U.2 | Do asset inventory and management processes include all physical objec... | N/A | Gaspar Labs maintains an inven... | 4 | 3.0 | 0 | 3.0 | 12 |
| U.2.1 | Are IoT devices identified by scanning for non-802.11 wireless technol... | - | - | 4 | 3.0 | 0 | 3.0 | 12 |
| U.2.2 | Is accountability for approval, monitoring, use and deployment of each... | - | - | 4 | 3.0 | 0 | 3.0 | 12 |

## V. Cloud Services

***Domain Baselines - Criticality: High | Impact: 4 | Likelihood: 3***

**Domain Risk: 12**

Evidence: -

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| V.1 | Are Cloud Hosting services provided? | No | Managed by Microsoft Azure. | 4 | 3.0 | 0 | 3.0 | 12 |
| V.1.1 | Is there a self-service portal available on the internet where clients... | - | - | 4 | 3.0 | 0 | 3.0 | 12 |
| V.1.3 | Is there a process approved by management to ensure that the Outsource... | Yes | Yes, backups for cloud-hosted ... | 4 | 2.5 | 0 | 2.5 | 12 |
| V.1.4 | Are backup image snapshots containing scoped data stored in an environ... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |
| V.2 | Does the Cloud Hosting Provider provide independent audit reports for ... | Yes | Gaspar Labs can provide our SO... | 4 | 2.5 | 0 | 2.5 | 12 |
| V.2.1 | Is the Cloud Service Provider certified by an independent third party ... | Yes | ISO 27001 and 27701 certificat... | 4 | 2.5 | 0 | 2.5 | 12 |
| V.3 | Are default hardened base virtual images applied to virtualized operat... | Yes | All virtual machine images are... | 4 | 2.5 | 0 | 2.5 | 12 |
| V.3.1 | Is the Service Provider responsible for ensuring the Guest Operating S... | Yes | All virtual machine images are... | 4 | 2.5 | 0 | 2.5 | 12 |

| # | Question | Resp | Add. Vendor Info | Imp | B.Lklhd | L.Adj | F.Lklhd | Risk |
|---|---|---|---|---|---|---|---|---|
| V.3.2 | Is the Service Provider responsible for deploying patches to the guest... | Yes | All virtual machine images are... | 4 | 2.5 | 0 | 2.5 | 12 |
| V.4 | Is the Cloud Service Provider responsible for deploying patches to the... | Yes | - | 4 | 2.5 | 0 | 2.5 | 12 |