# Monistax Risk and Compliance Assessment Report

## I. Risk Assessment

### 1. Operational Risk Scenarios

| RISK NO. | KNOWING | ENTERING | FINDING | EXPLOITING |
|---|---|---|---|---|
| 1 | SQL Injection | Attackers could craft SQL statements like admin’ OR ‘1’=’1’ to bypass authentication without a password | Locate valuable information (user records, sensitive configurations) within the database | Use database access to exfiltrate or modify data, compromising CIA. Disclosure of Banking Information |
| 2 | *Social engineering via phishing* | *Craft convincing emails that mimic legitimate sources, tricking users into clicking malicious links* | *Search for sensitive files or emails that store critical business information* | *Data leakage, use stolen credentials to access & extract confidential information and/or Alteration of payment information* |
| 3 | Cross Site Scripting XSS | If input fields do not validate input, attackers could use scripts that lead to session hijacking | Collects data from user sessions and cookies | Hijack user sessions or redirect users to phishing sites, risking credential theft |
| 4 | Brute Force Attacks | Automated scripts repeatedly make password attempts on user | Guesses weak or default passwords | Unauthorized access to user data & potentially Admin privileges |

| | | | | |
|---|---|---|---|---|
| | | accounts | | |
| 5 | Privilege Escalation | Exploits vulnerabilities for admin access, possible via SQL Injection | New privileges enable access to restricted sections | Modifications or actions within pose a risk to data integrity and confidentiality |
| 6 | Weak Encryption Practices | If sensitive data is not encrypted, attackers could intercept data in transit and at rest. | Sensitive data, like login credentials, are found in plain text | Access to unencrypted information such as payment information allows for data theft, undermining confidentiality |
| 7 | Data Leakage from Misconfigured Access Controls | Exploit overly permissive access controls to view or extract sensitive data | Sensitive files or directories are accessible without proper authentication | Confidential information is extracted, violating data protection policies |
| 8 | Distributed Denial of Service DDoS | Attackers can overwhelm the application with traffic | The system is unable to handle the excessive load | Web Server interruption affects availability, damaging reliability, and customer trust |
| 9 | Insufficient Logging and Monitoring | Stealthy access methods such as low-volume brute force or data scraping | Probing system components without being flagged | Long term access allows extensive data exfiltration or system manipulation unnoticed |
| 10 | Insecure API Endpoints | Exploit unprotected API endpoints or send crafted API request | Navigates through endpoints to locate sensitive resources | Unauthorized data retrieval can lead to Disclosure of banking Information affecting CIA |

## 2. Likelihood of Operational Scenarios

| Scenario | Strategic attack path | Overall likelihood |
|---|---|---|
| 1 | *Attacker identifies an injectable input field via vulnerability scans and injects SQL commands to bypass authentication* | *4 – Very Frequent* |
| 2 | Attackers gather employee information from social media, crafts convincing emails, deceives users into clicking malicious links or entering credentials on a fake page and uses credentials to access the system | 3- Frequent |
| 3 | Attacker identifies unfiltered input fields and injects malicious scripts to execute in other users browsers to gain access to sensitive information | 3- Frequent |
| 4 | Attacker identifies login endpoint and uses automated tools to repeatedly attempt passwords until successful & compromises user accounts, particularly those with weak passwords | 3- Frequent |
| 5 | Attackers gain low-level access through a compromised account and probe for privilege escalation vulnerabilities using SQL injection or misconfigurations to elevate privilege to admin | 2- Conceivable |
| 6 | Attackers intercept network traffic using packet capture tools to identify unencrypted data in transit to retrieve sensitive information such as credentials or personal data | 3- Frequent |
| 7 | Attackers navigate to sensitive files or directories and attempt to access resources directly through unprotected paths, retrieving sensitive information due to lack of proper authentication retrictions | 2- Conceivable |
| 8 | Attackers deploy a botnet and directs a high volume of requests to the target to overwhelm server resources, causing service outage | 2- Conceivable |
| 9 | Attackers perform low-volume, stealthy action probes for system weaknesses and go undetected due to lack of alerts or monitoring | 2- Conceivable |
| 10 | Attackers enumerate API endpoints via public documentation or scanning tools and send unauthorized requests to endpoints to retrieve or manipulate data without proper access controls | 3- Frequent |

## 3. Impact of Operational Scenario

| Scenario | Impact description | Impact score |
|---|---|---|
| 1 | Production Server (Customer & Financial Data). Legal & Financial impact if customer data is disclosed leading to Impacts on image and Trust | 4 |
| 2 | Human Resources Database. Financial impacts due to employee data exposure. | 2 |
| 3 | Customer Interaction Portal (software sales). XSS could result in session hijacking | 3 |
| 4 | Customer login system (software sales). Successful brute force attacks may compromise accounts impacting customer confidence with some financial implications | 2 |
| 5 | Production Server & Admis Access. Could attackers broad control over system data affecting operational integrity and media exposure | 4 |
| 6 | Database (Data in Transit). Weak encryption risks data interception, impacting brand trust & requiring internal corrective actions | 2 |
| 7 | Human Resources. Misconfigures controls could expose sensitive HR & financial data, leading to severe financial and legal consequences | 4 |
| 8 | Software services. Service disruptions due to DDoS attacks could result in customer complaints and limited financial loss due to downtime | 2 |
| 9 | Production & Database. Delayed detection of security breaches may allow data exfiltration & result in increased detection costs & operational impact | 3 |
| 10 | Customer & Accounting Database. Unsecured APIs may lead to unauthorized access & exposure of financial data, causing legal ramifications | 3 |

## 4. Risk Severity and Acceptance

| Scenario | Severity (matrix score) | Risk acceptance level |
|---|---|---|
| 1 | 4 x 4 = Matrix score 16 | High - Unacceptable |
| 2 | 3 x 2 = Matrix score 6 | Average - Tolerable under control |
| 3 | 3 x 3 = Matrix score 9 | Average - Tolerable under control |
| 4 | 3 x 2 = Matrix score 6 | Average - Tolerable under control |
| 5 | 2 x 4 = Matrix score 8 | Average - Tolerable under control |
| 6 | 3 x 2 = Matrix score 6 | Average - Tolerable under control |
| 7 | 2 x 4 = Matrix score 8 | Average - Tolerable under control |
| 8 | 2 x 2 = Matrix score 4 | Average - Tolerable under control |
| 9 | 2 x 3 = Matrix score 6 | Average - Tolerable under control |
| 10 | 3 x 3 = Matrix score 9 | Average - Tolerable under control |

## 5. Risk Prioritization

| Scenarios in order of priority (highest -> lowest priority) |
|---|
| SQL Injection |
| Insecure API Endpoints |
| Cross-Site Scripting (XSS) |
| Data Leakage from Misconfigured Access Controls |
| Privilege Escalation |
| Brute Force Attacks |
| Weak Encryption Practices |
| Insufficient Logging |
| Social Engineering |
| Distributed Denial of Service (DDoS) |

# 6. Recommended Actions

| Risk scenario | Security measure | Difficulties for implementation | Timeframe *(choose one: short-term, mid-term, long-term)* |
|---|---|---|---|
| 1 | Implement parameterized SQL statements & input validation on all user inputs. Conduct routine security audits for SQL vulnerabilities. | Significant development resources required for code review and refactoring. Testing is essential but time intensive. | Short-term (Immediate priority) |
| 2 | Secure API endpoints with authentication, rate limiting, and logging. Use an API gateway for control over API access and security checks. | May require reconfiguration of existing APIs. Integration of gateway may need additional development and testing | Short-term |
| 3 | Apply input sanitization and content security policy (CSP) to prevent script execution. Regularly scan for XSS vulnerabilities. | Legacy code updates can be challenging and time consuming. Requires developer commitment to test sanitization thoroughly. | Short-term |
| 4 | Enforce least privilege access controls and conduct regular access reviews to ensure permissions are correctly configured. | Access control reviews require coordination across departments. Audits need consistent scheduling and follow up. | Short-term |
| 5 | Implement Role-Based access (RBAC) to limit access based on roles, and monitor privilege changes. Regularly audit permissions. | Requires thorough review of current permissions and potential restructuring of access hierarchy. RBAC setup may require custom configuration. | Short-term |
| 6 | Enforce rate limiting, account lockout | Balancing security with user convenience is | Mid-term |

| | | | |
|---|---|---|---|
| | mechanisms, and strong password policies. Monitor for unusual login attempts to detect brute force activity. | challenging, and overly strict settings can disrupt user experience. | |
| 7 | Enforce strong encryption protocols for data in transit (TLS 1.2 or higher) and at rest (AES-256). Regularly review encryption standards for compliance. | Updating encryption can impact system performance. It may also require hardware upgrades if legacy systems are incompatible. | Mid-term |
| 8 | Implement centralized logging and monitoring with SIEM (Security Information and Event management) integration. Set up alerts for unusual activity patterns. | SIEM setup is costly and requires skilled personnel to manage and avoid alert fatigue. Tuning may be complex. | Mid-term |
| 9 | Conduct security awareness training focused on phishing recognition and reporting. Implement multi-factor authentication (MFA) to reduce credential theft risks. | Security awareness training must be ongoing for maximum effectiveness. MFA setup may temporarily disrupt workflows. | Mid-term |
| 10 | Deploy a web application firewall (WAF) and DDoS protection service. Implement load balancing and monitor for traffic anomalies. | DDoS mitigation services can be costly. Ensuring security without affecting performance is challenging. | Mid-term |

# 7. Conclusion

After conducting a thorough risk assessment of the software solution, we identified several critical vulnerabilities, including SQL Injection, Insecure API Endpoints, and Privilege Escalation. Each of these poses a significant risk to Monistax’s core mission of ensuring data confidentiality, integrity, and availability, especially given the high potential for exploitation and the critical impact on customer data. Additional vulnerabilities, such as Cross-Site Scripting (XSS) and Weak Encryption Practices, are also present and require structured controls to mitigate. Overall, these risks are manageable but will require proactive and consistent security measures.

Given the identified risks, I recommend adopting the software only if Monistax implements a robust security plan to address the high priority vulnerabilities. Essential actions include securing API endpoints, enforcing strong input validation, implementing parameterized queries to prevent SQL Injection, applying centralized logging and monitoring, and conducting regular security training. Monistax should also allocate resources for continuous security audits, particularly around access control and logging. These actions will help mitigate immediate risks and sustain secure operations. Implementing these security controls may incur costs and require initial adjustments in workflow but is essential for ensuring long term, secure usage of the solution.

# II. Compliance Assessment

## 1. Discrepancies

*The security scan revealed a SQL injection vulnerability that allowed administrative access without credentials, which conflicts with Monistax's requirement for secure, limited access to data and prevention of unauthorized database interactions.*

*While Monistax's policy requires strong encryption there is no evidence from the PeoplePro documentation confirming adherence to these encryption standards.*

*Monistax's policy mandates a logging mechanism to track access and events for auditability, but the documentation lacks detail on whether PeoplePro Suite logs user activities or maintains detailed access logs.*

*Monistax's policy recommends strong authentication, ideally multi-factor authentication, but the PeoplePro Suite appears to rely solely on basic username and password authentication.*

*Monistax requires that SaaS providers store customer data within the EEA, but there is no information in the PeoplePro documentation specifying data storage location compliance.*

*Monistax's policies emphasize strict access control and role-based permissions. PeoplePro's documentation does not clearly outline any role-based access control (RBAC) system or other permission structures to restrict access based on user roles.*

## 2. Source of Discrepancies

| Discrepancy | Source: solution or policy? |
|---|---|
| 12.2 Vulnerability Prevention | Missing Section in Monistax Policy |
| Information Security Policy | Missing Section in Monistax Policy |
| *SQL Injection* | *Automated Security Scan* |
| *Lack of Strong Encryption* | *Appendix to Monistax Third-Party Supplier Security Policy: SaaS* |
| *Insufficient Logging & Monitoring* | *Monistax Third-Party Supplier Security Policy* |
| *No Multi Factor Authentication* | *Monistax Third-Party Supplier Security Policy* |
| *Data Location Unclear* | *Monistax Third-Party Supplier Security* |

| | *Policy* |
|---|---|
| *Access Control & Role Bases Permissions* | *PeoplePro Suite: Description and Terms & Conditions* |

## 3. Recommendations: Solution

| Flaw | Action | Justification |
|---|---|---|
| *Information Security Policy Requirement* | *Require third-party providers to submit a comprehensive Information Security Policy* | *An Information security Policy demonstrates commitment to security standard* |
| *SQL Injection* | *Use parameterized SQL queries & input validation* | *Prevents Injection attacks & ensures secure database interactions* |
| *Lack of Strong Encryption* | *Enforce TLS 1.2+ for data in transit & AES-256 for data at rest* | *Protects data confidentiality and meets Monistax's encryption standards* |
| *Insufficient Logging & Monitoring* | *Implement centralized logging for access and event tracking* | *Enhances traceability and supports incident response* |
| *No Multi Factor Authentication* | *Add MFA for all accounts especially admin users* | *Strengthens authentication, reducing risk of unauthorized access* |
| *Data Location Unclear* | *Specify data storage locations in compliance with EEA requirements* | *Ensures data residency compliance and regulatory alignment* |
| *Access Control & Role Bases Permissions* | *Implement RBAC and regularly review permissions* | *Limits access based on role, enhancing data security* |

## 4. Recommendations: Updates or Corrections to Policy

| Section of policy or document to be modified | Suggested Modification | Justification |
|---|---|---|
| Third-Party Supplier | Require all third-party | Ensures baseline security |

| | | |
|---|---|---|
| Security Policy - Documentation Requirements | providers to submit an Information Security Policy covering core areas like data protection, access control & incident response | practices, addressing a key gap found in PeoplePro Suite. |
| Third-Party Supplier Security Policy - Encryption Requirements | *Specify minimum encryption standards* | *Clear standards prevent uncertainty and ensure all suppliers meet Monistax's encryption requirements consistently* |
| Third-Party Supplier Security Policy - Access Controls | *Require role-based access control as a standard for all third-party solutions* | *RBAC ensures that only authorized users access sensitive data, supporting the principle of least privilege* |
| Appendix - Data Residency | *Include specific guidelines on approved data residency locations beyond the EEA, if any, and clarify requirements for location disclosure* | *Clear location requirements reduce uncertainty and help ensure data compliance with Monistax's regulatory obligations* |
| Third-Party Supplier Security Policy - Authentication Standards | *Add a requirement for multi-factor authentication for high-privilege accounts* | *MFA strengthens authentication security, reducing the risk of unauthorized access through compromised credentials* |
| Appendix - Logging and Monitoring | *Specify that third-party solutions must have centralized logging with event tracking for access and security incidents* | *This requirement enhances visibility and supports Monistax's auditing and incident response capabilities* |

These modifications help ensure that Monistax's policies clearly define security requirements, reducing ambiguity and improving third-party compliance with critical security practices.