Monistax

Monistax Risk and Compliance Assessment Report

I. Risk Assessment

1. Operational Risk Scenarios

RISK NO.	KNOWING	ENTERING	FINDING	EXPLOITING
1	The attacker identifies the login page of the PeoplePro Suite.	They inject a malicious SQL command into a form field.	They gain administrative-level access to the HR system.	They exfiltrate or tamper with employee personal and financial data.
2	The attacker finds a public login portal.	They use brute-force or credential stuffing techniques.	They gain access to a legitimate user account.	They read or alter sensitive employee records.
3	The attacker sends a phishing email to an employee.	The employee clicks the link and enters their credentials on a fake site.	The attacker logs in using the stolen credentials.	They view or modify payroll and contract data.
4	The attacker scans cloud resources for misconfigurations.	They find and access an unsecured storage bucket.	They access HR documents stored in the cloud.	They leak confidential employee data online.
5	The attacker has already breached the system.	Due to unclear SLA obligations, the vendor does not report the breach.	The attacker remains in the system undetected.	They continue extracting sensitive data over time.
6	The attacker captures session tokens on an	They replay the session token to gain access.	They impersonate an admin session.	They modify system

	unsecured network.			configurations or steal data.
7	A disgruntled employee realizes they have excess permissions.	They access areas of the system beyond their role.	They locate sensitive HR or payroll data.	They manipulate or leak this data out of spite.
8	The attacker sets up a fake public Wi-Fi network.	An employee connects and logs in without VPN protection.	The attacker captures login credentials in transit.	They later use the credentials to access the system.
9	The vendor retains old archived data post-contract.	An attacker compromises the vendor's system.	They find outdated HR files still stored.	They publish or monetize the breached data.
10	The attacker runs probes on the application.	They find flaws but no alerts or logs capture the activity.	They stay in the system undetected.	They alter or delete critical records without being discovered.

2. Likelihood of Operational Scenarios

Scenario	Strategic attack path	Overall likelihood
1	The attacker discovers the login page and injects a SQL payload into a vulnerable input field, bypassing authentication to gain administrative access.	4 – Likely
2	The attacker identifies a public-facing login portal and uses credential stuffing or brute-force attacks to gain access by exploiting weak user passwords.	3 – Frequent
3	The attacker sends a phishing email to a user, successfully captures credentials, and accesses the account due to the absence of multi-factor authentication.	4 – Very frequent

4	The attacker scans for misconfigured cloud storage and locates an unsecured storage bucket or database, allowing them to retrieve exposed files.	3 – Frequent
5	A breach occurs, but due to unclear SLA terms, the vendor fails to notify Monistax promptly, allowing the exposure to persist undetected.	2 – Conceivable
6	The attacker intercepts session tokens on an unsecured network and replays them to impersonate an administrative user.	3 – Frequent
7	An insider discovers they have elevated privileges and uses them to access restricted HR or financial data, which they then modify or leak.	3 – Frequent
8	The attacker monitors public Wi-Fi traffic, intercepts credentials during user login, and reuses those credentials to access the system.	2 – Conceivable
9	The vendor retains archived data after the contract ends, and an attacker breaches the vendor's system to access outdated but still sensitive records.	2 – Conceivable
10	The attacker probes the system for weaknesses. Due to the absence of audit logs or alerts, their abnormal activity goes unnoticed, enabling data tampering or deletion.	3 –Frequent

3. Impact of Operational Scenarios

Scenario	Impact description	Impact score
1	A successful SQL injection could compromise the entire HR database, exposing personal and financial data of all employees, resulting in major legal and financial consequences.	5 – Very High
2	Brute-force access to employee accounts could lead to unauthorized viewing or alteration of HR data, affecting employee privacy and trust.	4 – High
3	Phishing without MFA could result in widespread unauthorized access, payroll fraud, and reputational damage if multiple employee accounts are compromised.	4 – High

4	Misconfigured cloud storage could expose confidential employee documents and contracts to the public, leading to regulatory violations and loss of trust.	4 – High
5	A delayed breach notification could worsen the damage, allowing attackers extended access and increasing the chances of legal penalties for non-compliance.	4 – High
6	Session hijacking could result in administrative control being taken over by attackers, leading to unauthorized changes, data leaks, or lockouts.	3 – Moderate
7	An insider with excessive privileges could access or alter sensitive information, disrupting payroll operations and potentially causing legal issues.	3 – Moderate
8	Attacks via public Wi-Fi could lead to credential theft and account breaches, especially if employees log in without secure connections.	2 – Low
9	Archived data breaches could leak outdated but still sensitive information, violating data protection laws and damaging public trust.	3 – Moderate
10	A lack of audit logs could prevent timely detection of attacks, allowing tampering to go unnoticed and undermining incident response efforts.	4 – High

4. Risk Severity and Acceptance

Scenario	Severity (matrix score)	Risk acceptance level
1	20 (4 x 5)	Not Acceptable
2	12 (3 x 4)	Borderline Acceptable
3	16 (4 x 4)	Not Acceptable
4	20 (3 x 4)	Not Acceptable
5	8 (2 x 4)	Acceptable

6	9 (3 x 3)	Borderline Acceptable
7	9 (3 x 3)	Borderline Acceptable
8	8 (2 x 4)	Acceptable
9	6 (2 x 3)	Acceptable
10	12 (3 x 4)	Borderline Acceptable

5. Risk Prioritization

Scenarios in order of priority (highest -> lowest priority)
Scenario 1 is the highest priority because a successful SQL injection could give attackers administrative access, leading to the exposure of highly sensitive HR data.
Scenario 3 is also critical, as phishing attacks can easily bypass weak authentication and result in major data breaches involving payroll or employee information.
Scenario 2 is still a significant risk because it targets weak authentication practices. If successful, attackers could gain access to employee accounts and potentially escalate privileges, especially in the absence of strict account lockout policies
Scenario 4 involves accidental exposure of HR files through unsecured storage buckets or databases. Given the sensitivity of HR data, even one instance of misconfiguration could result in large-scale data leaks.
Scenario 10 is prioritized closely behind because the absence of proper logging can delay detection of malicious activity. This enable attackers to remain undetected for extended periods, increasing the potential for data manipulation or destruction.

Scenario 6 presents session hijacking allows attackers to impersonate administrative users. This could lead to unauthorized changes, data theft, or complete system compromise if not promptly addressed.
Scenario 7 is where insider risk is particularly dangerous because it originates from within the organization. A malicious or careless insider could abuse elevated permissions to leak, delete, or alter sensitive payroll or HR information.
Scenario 5 is a moderate concern because a vendor's failure to notify Monistax of a breach would delay incident response and potentially worsen the damage.
Scenario 9 ranks low but is still worth addressing; if old archived data is not deleted after contract termination, it could be compromised later through vendor breaches.
Scenario 8 is the lowest priority, as credential interception over public Wi-Fi is less likely with proper user training and VPN usage, though it still poses a potential access risk.

6. Recommended Actions

Risk scenario	Security measure	Difficulties for implementation	Timeframe *(choose one: short-term, mid-term, long-term)*
1	Deploy a web application firewall (WAF) and conduct regular security testing.	May require infrastructure changes and budget approval.	Short-term
2	Implement account lockout policies and CAPTCHA systems to deter brute-force attacks.	Could disrupt user experience if thresholds are too strict.	Short-term

3	Enforce multifactor authentication (MFA) for all users and conduct phishing awareness training.	User resistance or confusion about MFA setup may delay full adoption.	Short-term
4	Audit cloud infrastructure configurations and remediate misconfigurations.	Requires cloud expertise and full access to third-party environments.	Mid-term
5	Clarify breach notification terms in all SLAs.	Requires renegotiation with vendors and legal review.	Mid-term
6	Apply strong session management policies, including encrypted tokens and session timeouts.	May involve development work and require updates to existing applications.	Short-term
7	Review user roles periodically and enforce least privilege access.	May require HR collaboration and auditing tools.	Mid-term
8	Provide employee training on safe network use and require VPN for remote access.	Some users may lack awareness or technical ability to configure VPNs.	Short-term
9	Enforce vendor data retention and deletion policies.	Depends on vendor cooperation and shared legal responsibilities.	Long-term
10	Enhance system logging and implement monitoring for suspicious activity.	May require SIEM integration and increased resource allocation for monitoring.	Mid-term

7. Conclusion

The assessment of the PeoplePro Suite identified several high and critical severity risks that exceed Monistax's acceptable risk threshold, including vulnerabilities such as SQL injection, phishing attacks, session hijacking, and insufficient logging. These issues, if exploited, could significantly impact the confidentiality, integrity, and availability of sensitive HR data, resulting in potential legal, financial, and reputational consequences for the organization.

From a compliance standpoint, PeoplePro Suite meets some but not all of Monistax's third-party supplier security requirements. Notable gaps were found in breach notification timelines, data retention and deletion policies, and enforcement of least privilege access. Adoption of the solution should only proceed if these Not Acceptable and Borderline Acceptable risks are mitigated through stronger access controls, secure configurations, multifactor authentication, enhanced monitoring, and contractual updates with the vendor. With these measures implemented and verified, PeoplePro Suite could be safely integrated with a reduced residual risk profile.

II. Compliance Assessment

1. Discrepancies

- The Monistax Third-Party Supplier Security Policy requires that all vendors provide a documented security policy to outline their security measures, controls, and governance practices. This requirement is not met, as no such policy is included in the PeoplePro Suite: Description and Terms & Conditions.
- Clause 12.2 on vulnerability prevention, as specified in the Monistax Third-Party Supplier Security Policy: SaaS appendix, is absent from the vendor's documentation. This clause outlines proactive measures to identify, mitigate, and remediate vulnerabilities, which are critical for maintaining security.
- The PeoplePro Suite documentation does not specify data retention timelines or secure deletion protocols for customer data after contract termination, which could lead to non-compliance with Monistax's data protection requirements.
- The vendor's breach notification procedures do not align with Monistax's policy on notification timelines, potentially delaying the company's incident response and increasing exposure to risk.

2. Source of Discrepancies

Discrepancy	Source: solution or policy?
Lack of a Third-Party Security Policy	Monistax Third-Party Supplier Security Policy
Missing Vulnerability Prevention Clause	Monistax Third-Party Supplier Security Policy: SaaS Appendix (Clause 12.2)
Data retention and Deletion Gaps	Monistax Third-Party Supplier Security Policy
Breach Notification Timeline	Monistax Third-Party Supplier Security Policy

3. Recommendations: Solution

Flaw	Action	Justification
No MFA	Require implementation of MFA for all users	Prevents unauthorized access from stolen passwords
No encryption mentioned	Mandate encryption for data at rest and in transit	Ensures confidentiality and aligns with best practices
SQL injection vulnerability	Patch immediately using input validation and parameterized queries	Critical vulnerability—direct access to admin
No breach notification process	Require clear SLA clause on breach disclosure within 72 hours	Regulatory and reputational protection
Data residency unclear	Require vendor to disclose where data is stored and processed	Needed for GDPR/CCPA compliance
No user role descriptions	Enforce least privilege and role-based access control	Prevents insider misuse or accidental exposure
No logging/audit trail	Add activity logging with regular reviews	Needed for incident response and accountability
No third-party audit proof	Ask for SOC 2 / ISO 27001 or recent security audit	Verifies vendor maturity and trustworthiness

4. Recommendations: Updates or Corrections to Policy

After reviewing both Monistax policy docs, we did **not** find a flaw in Monistax's policies that led to the above issues. However, here are two optional policy enhancement suggestions:

Section of Policy	**Suggested Modification**	**Justification**
Third-Party Policy – Logging	Require vendors to provide access to log records on request	Improves transparency and incident forensics

SaaS Appendix – Certifications	Add requirement to provide proof of current third-party security certification	Helps verify vendor's security claims

Sources

1. **Monistax Risk Management Policy** (Version 2). Monistax Internal Documentation.
2. **Monistax Standard Operating Procedure: Risk Management** (Version 2). Monistax Internal Documentation.
3. **Monistax Risk Management Scales** (Version 2). Monistax Internal Documentation.
4. **Monistax Third-Party Supplier Security Policy** (Version 2). Monistax Internal Documentation.
5. **Appendix to Monistax Third-Party Supplier Security Policy: SaaS** (Version 2). Monistax Internal Documentation.
6. **Monistax Values** (Version 2). Monistax Internal Documentation.
7. **PeoplePro Suite: Description and Terms & Conditions** (Version 2). Vendor Documentation.
8. **Automated Security Scan of PeoplePro Suite** (Version 2). Vendor Documentation.
9. **Documentation Use Guide** (Version 2). Monistax Internal Documentation.
10. **Cuelogic.** “How to Make Sense of Cybersecurity Frameworks.” Retrieved from: https://www.cuelogic.com/blog/cybersecurity-frameworks
11. **Course: Discover the World of Cybersecurity.** Chapters: *Discover the World of the Attackers*, *Discover How Cybersecurity Professionals Work Together*, and *Understand How Organizations Manage Cybersecurity Priorities*.