Cloud-Based HRMS Risk Register (Mapped to NIST CSF)

Risk ID	Description	Vulnerability	Impact	Likelihood	Risk Score	Owner	Status	NIST CSF Category	Mitigation Actions
RR-001	Orphaned IAM accounts could be exploited after staff offboarding	Weak IAM lifecycle management	High	Medium	Medium-High	IT Security Manager	Open	Protect	Implement automated de-provisioning linked to HR offboarding; conduct quarterly IAM account reviews.
RR-002	Privilege abuse possible due to overlapping HR/payroll roles	Lack of separation of duties	High	Medium	Medium-High	Security Engineer	Open	Protect	Enforce RBAC and SoD policies; review and segregate conflicting roles.
RR-003	Excessive AWS permissions increase attack surface	Overly broad IAM policies	High	High	High	IAM Admin	In Progress	Protect	Conduct IAM permissions audit; enforce least privilege; use permission boundaries.
RR-004	Brute force attack risk due to no account lockout policy	Weak authentication configuration	High	Medium	Medium-High	App Dev Team	Open	Protect	Configure account lockout thresholds; enable MFA on all accounts.
RR-005	Incomplete logs may hinder forensic investigations	Missing metadata in audit logs	Medium	Medium	Medium	App Dev Team	In Progress	Detect	Enable full logging including metadata; standardize log formats; store in centralized logging solution.
RR-006	Undetected malicious activity due to no log reviews	Lack of audit log monitoring	High	High	High	SOC Manager	Open	Detect	Implement scheduled log reviews; configure automated alerts for suspicious events.
RR-007	Audit logs could be deleted or altered	Insufficient S3 bucket protections	High	Medium	Medium-High	S3 Admin	In Progress	Protect	Enable S3 Object Lock and MFA Delete; restrict access to log

									storage buckets.
RR-008	Inability to link actions to individuals	Shared admin accounts without MFA	High	Medium	Medium-High	IAM Admin	Open	Protect	Eliminate shared accounts; enforce MFA for all privileged accounts.
RR-009	HR staff unaware of privacy handling requirements	No privacy awareness training	Medium	Medium	Medium	Privacy Officer	Planned	Protect	Conduct mandatory privacy and data handling training; track completion in LMS.
RR-010	Developers lack secure coding skills	No role-based security training	High	Medium	Medium-High	Security Manager	Planned	Protect	Provide secure coding training; conduct annual refreshers and code review sessions.
RR-011	Unidentified emerging threats due to outdated risk assessment	Stale risk assessment process	High	Medium	Medium-High	Risk Officer	Open	Identify	Update risk assessment annually; integrate threat intelligence feeds into process.
RR-012	Unpatched vulnerabilities in Lambda functions	No vulnerability scans	High	Medium	Medium-High	Security Engineer	Open	Protect	Implement regular serverless code scanning; integrate into CI/CD pipeline.
RR-013	Increased exploit risk due to delayed patching	Patching not within policy timelines	High	High	High	Systems Admin	In Progress	Protect	Enforce patch SLAs; automate patch deployment and verification.
RR-014	Delayed incident detection due to lack of SIEM integration	GuardDuty alerts not centralized	High	High	High	SOC Analyst	Open	Detect	Integrate GuardDuty with SIEM; enable real-time alerting and incident workflows.