Table of Contents

RMF Implementation for a Cloud-Based HR Management System

Objective:

Demonstrate practical application of the NIST Risk Management Framework (RMF) steps using a fictional cloud-based system that manages sensitive but unclassified data (FISMA Moderate level). Showcase how selected NIST 800-53 controls are implemented, assessed, and monitored.

Project Components (RMF Steps):

1. Categorize the System

- **System Name:** Cloud -based HR Management System (HRMS)
- **Information Types:** Employee, payroll data, PII, onboarding/ offboarding workflows
- **Impact Level:** Moderate (FIPS 199)
- **Deliverable:** System Categorization Report

2. Select Security Controls

- **AC-Access Control**
  - **AC-2: Account Management –** Define and document the accounts authorized to access and modify data. Use IAM for Role-based access controls.
  - **AC-5: Separation of duties –** Reduce risk of fraud and conflict of interest. Ensure job rotation. No single individual performs a process end-to-end i.e, salary changes are approved by a senior. Divide responsibilities
  - **AC- 6: Least Privilege –** Data minimization and access control. Minimum permissions necessary to complete job function. Minimize risk exposure in the event of a compromise to a specific account.
  - **AC-7: Unsuccessful Log-on Attempts –** Prevent brute force attempts. Detect potentially compromised accounts.
- **AU – Audit and Accountability.**
  - **AU-3: Content of Audit Records –** Audit events must capture sufficient detail to show changes, including user ID and timestamps, to ensure changes made were authorized.
  - **AU-6: Audit Review, Analysis, and Reporting -** Regular review and analysis of audit logs are essential for detecting anomalies and compliance violations
  - **AU-9: Protection of Audit Information –** Audit records provide a trail of information and should be protected from any modifications, deletion or unauthorized access, as evidence needs to be admissible in court.
  - **AU-10: Non-Repudiation –** Actions taken are linked to an individual to ensure accountability for sensitive actions like payroll processing.

- **AT – Awareness and Training**
    - **AT-2: Security Awareness Training –** Regular training of users on ways to recognize and prevent data breaches and improper data handling procedures.
- **RA – Risk Assessment**
    - **RA-3: Risk Assessment –** Comprehensive risk assessment identifies threats, vulnerabilities and impacts to the system. Supports selection and prioritization of controls.
    - **RA-5: Vulnerability Monitoring and Scanning –** Regular scheduled scanning helps detect known vulnerabilities to protect system from exploits
- **SI – System and Information Integrity**
    - **SI-2: Flaw Remediation –** Timely identification and patching of vulnerabilities to protect the system from exploitation
    - **SI-4: System Monitoring –** Monitoring system behaviour to detect anomalies including early IOCs, policy violations and unauthorized behaviour. This ensures system and data integrity
- **Deliverable:** Security Control Selection Document

3. System Security Plan

- **AC-2**
    - **AC-2: Account Management –** Use IAM for RBAC.
    - **AC-5: Separation of duties –** Senior role above the role making the request is the approver. Separate accounts used to privileged activities for admins.
    - **AC- 6: Least Privilege –** SCPs with AWS Organizations for fine-grained access controls i.e prevent developers from accessing production. AWS Config to monitor config rules against defined organization rules, AWS KMS to manage encryption keys
    - **AC-7: Unsuccessful Log-on Attempts –** Password attempt restrictions
- **AU – Audit and Accountability.**
    - **AU-3: Content of Audit Records –** Audit events must capture sufficient detail to show changes, including user ID and timestamps, to ensure changes made were authorized.
    - **AU-6: Audit Review, Analysis, and Reporting -** Regular review and analysis of audit logs are essential for detecting anomalies and compliance violations
    - **AU-9: Protection of Audit Information –** Audit records provide a trail of information and should be protected from any modifications, deletion or unauthorized access, as evidence needs to be admissible in court.
    - **AU-10: Non-Repudiation –** Actions taken are linked to an individual to ensure accountability for sensitive actions like payroll processing.
- **AT – Awareness and Training**
    - **AT-2: Security Awareness Training –** Regular training of users on ways to recognize and prevent data breaches and improper data handling procedures.

Different groups, including finance, HR and sys admins have access to HRMS. It is vital to tailor training to their interaction with the system.

- **RA – Risk Assessment**
  - **RA-3: Risk Assessment –** Use AWS Well-Architected Tool, Threat Modelling Exercise using MITRE ATT&CK Framework, Maintain a risk register, Document periodic **risk assessments** in line with FIPS 199 and FIPS 200, customized to HRMS data sensitivity (e.g., PII, payroll).
  - **RA-5: Vulnerability Monitoring and Scanning –** Use AWS System Manager for Patch Management, Nessus/ Tenable for deeper scans, Amazon Inspector for EC2 instances and containers
- **SI – System and Information Integrity**
  - **SI-2: Flaw Remediation –** Patch Manager through AWS System Manager for automatically apply security patches, AWS Security hub to consolidate findings across different AWS services, Create a patch schedule to remediate any exceptions.
  - **SI-4: System Monitoring –** Use CloudTrail to monitor and audit changes, Utilize logging tools to collect logs including VPC Flow logs, CloudWatch logs. Set up GuardDuty for threat intel, Set up CloudWatch alarms for unusual activities.
- **Deliverable:** Security Implementation Plan (with screenshots or diagrams)

---

4. Security Assessment Report

a. AC-2

Method:

- Examine IAM Policies and user life cycle procedures
- Cloudtrail logs to trace IAM log activities
- Correlate user requests made to the ticketing system to actions performed by admins
- Manual review through interviews with HR and IT admins: “Kindly take me through the process from onboarding to user termination?”
- Create a dummy user and test for multi-factor authentication

Evidence:

- A dummy user was used to simulate the creation and termination policy in production. The user was given least privilege and clean up was done afterwards.
- IAM policies and Cloudtrail logs were reviewed

Status:

- Existing IAM accounts for staff that left the organization

b. AC-5

Method:

- Examine company policies on job rotation
- SoD matrix to find incompatible permissions
- IAM role definitions for employees i.e. What does a certain role do?
- Conduct interviews with IT admins: “How to you prevent a single user from having conflicting responsibilities?”. Examine IAM roles and permissions to ensure that permission boundaries and RBAC are enforced
- Examine the ticketing system for approvals to ensure the person conducting the activity does not also approve for themselves to perform it.
- Attempt to perform non-privileged and privileged activities using the same account

Evidence:

- Review ticketing system process flow from the time a request is made, to its approval to its action.
- Review SoD Matrix
- Interview results
- IAM logs
- Privileged activities can be performed using a normal admin account

Status:

- Overlap of roles i.e a HR admin performed multiple actions which could increase risk of fraud and error
- The role matrix is outdated and needs an update.
- Unclear company policies on job rotation
- Lack of separate admin accounts for performing privileged and non-privileged activities

c. AC-6

Method:

- Review IAM users and policies
- Resource based policies
- AWS Config rules
- IAM Access Analyzer logs

Evidence:

- Select a sample user or role and verify that they can only perform actions specific to their roles and no extra permissions are assigned to their user.
- Attempt to perform unauthorized actions like deleting a user for a user for non-admin accounts in a test environment.

Status:

- IAM policies use wildcards granting excessive privileges to users

d. AC-7

Method:

- Simulate failed log on attempts
- Review Cloudtrail and CloudWatch logs for failed authentications
- IAM policies

Evidence:

- Review password policies
- Review account lockout policy
- Review GuardDuty findings to see if it captured the activity

Status:

- High account lockout threshold due to poor policy. Users can retry failed password attempts up to 5 times within a short period of time. Increases risk of brute-force attacks
- Poor password policy. This allowed users to create insecure passwords that allowed short passwords up to 5 characters, no password complexity, no maximum password age.

e. AU-3

Method:

- Review audit logs to confirm that sufficient detail to support investigations and accountability is captured
- Review the log format. Check for relevant fields, including user ID, event type, timestamp, affected resource
- Perform a test action e.g. an update or a log in attempt and verify the log has been captured and logged correctly with metadata

Evidence:

- Review Cloudtrail logs
- Review Cloudwatch logs
- Review OpenSearch Dashboards

Status:

- Logs missing IP address field for certain user activities

f. AU- 6

Method:

- Review Standard Operating Procedures (SOPs)

- Review historical audit review reports
- Review policies on internal audit reviews
- Review findings from previous audits
- Conduct interviews to confirm that audit logs are reviewed regularly and, if used for security findings: “Who reviews the logs and how often? What actions are taken from log findings?

Evidence:

- Review Cloudtrail logs
- Review Cloudwatch logs
- Review OpenSearch Dashboards
- Review Security Hub

Status:

- Outdated SOPs
- Irregular review of audit logs not in line with company policies
- Lack of audit review reports

g. AU-9

Method:

- Examine IAM roles and policies controlling access to logs
- Review S3 bucket policies
- Encryption settings for logs
- Attempt to modify a log file and use CloudTrail log file integrity validation to review if the change is captured
- Ensure MFA Delete is enabled for delete actions to ensure logs are protected from unauthorized or accidental deletion.

Evidence:

- Review IAM policies
- Review S3 Policies
- Review CloudTrail logs
- Review KMS Settings

Status:

- Cleanup needed on roles that have access to logs. Limit to admins and not all HR admins which is the case currently
- Audit logs stored in S3 without proper bucket-level restrictions

h. AU-10

Method:

- IAM roles with MFA Enforcement
- Review logs to show unique user actions
- Perform a privileged action and check logs to confirm its traceable to an identity
-

Evidence:

- Review IAM policies and roles to ensure MFA is enforced
- Cloud Trail Logs

Status:

- Privileged admin actions not tied to individual identities

i. RA-3

Method:

- Examine most recent Risk Assessment Report
- Review Risk Register for open and closed risks
- Review Guardduty for potential threats and malicious activity
- Conduct interviews with risk officer, security lead and system owner
- Threat Modelling Exercise
- AWS Well-Architected tool

Evidence:

- Risk Assessment Report
- Risk Register
- Guardduty logs
- Review SOPs
- Review Well-Architected Tool findings

Status:

- Risk register is not updated to match the current situation. Open findings have not been recorded and closed findings are still open in the register.

j. RA-5

Method:

- Use AWS Systems Manager Patch Manager to run a compliance scan
- Run Amazon Inspector on an EC2 instance and review findings
- Review scan schedules
- Review scan results from custom VAPT scan software like Nessus
- POA&M Report for vulnerabilities found but not yet remediated

Evidence:

- Inspector scan reports
- Nessus scan report
- Patch Manager results
- Review POA&M entries

Status:

- POA&M has vulnerabilities that are yet to be patched within the organization's patch timeframe, increasing the probability of threats being exploited by attackers.

k. SI-2

Method:

- Review Patch Management Policy and documented timelines for applying patches
- Review patch results and compliance reports from Patch Manager
- Security Hub findings

Evidence:

- Security Hub Report
- Patch Manager Reports
- Policy and timeline documentation

Status:

- Vulnerabilities not patched within timelines

l. SI-4

Method:

- Simulate a security event
- Verify CloudTrail, GuardDuty and CloudWatch events for any entries that match the simulated event

Evidence:

- CloudTrail Logs
- CloudWatch Logs
- Monthly monitoring and incident response alerts
- Guardduty Logs

Status:

- GuardDuty and CloudTrail logs not integrated into SIEM

m. AT-2

Method

- Review training policy schedule

- Review latest training materials for their relevance and currency
- Attendance records
- Course completion records and test results
- Onboarding checklist – Check if security awareness training is included
- Conduct interviews

Status

- No formal security awareness training plan

5. Plan of Action & Milestones (POA&M)

Weakness ID	Description	Controls Affected	Corrective Actions	Milestones	Resources Required	Completion Date	Status
POAM 01	IAM accounts not deleted for exited staff	AC-2	• Automated provisioning and deprovisioning of accounts via AWS Identity Center • Proper user onboarding and offboarding policies and procedures • HR-IT Workflow Integration	Design, test and implement automation in Identity Center, policies and interdepartmental workflow integration.	IAM Admin HR Admin	2025-09-15	Open
POAM 02	HR roles with overlapping increasing risk of fraud and errors.	AC-5	• Review and update SoD Matrix • Review IAM roles definitions and their permissions	Review IAM roles and their permissions Redesign role definitions Apply and veriffy policy updates	IAM Admin HR Lead	2025-09-30	Open
POAM 03	IAM policies use wildcards granting excessive privileges	AC-6	• Apply least privilege using RBAC	Policy audit Remove wildcards Test and implement changes	IAM Admin	2025-08-31	Ongoing

POAM 04	Poor password policy	AC-7	• Configure a password policy with restrictions that allow users to create a strong password which reduces risk of brute force attempts	Policy review Config update Test, deploy and enforce	IAM Admin	2025-09-10	Open
POAM 05	Audit logs missing IP address for certain user activities	AU-3	• Update logging data to include all relevant metadata	Log config update Test and deploy logging settings	App Dev Team	2025-08-25	In Progress
POAM 06	Irregular review of logs	AU-6	• Update the SOP to include a documented monthly log review and assign log review owners	Update existing SOP Train staff Test, implement and review schedule	Security Team Security Lead	2025-09-20	Open
POAM 07	Audit logs stored in S3 without bucket level permissions	AU-9	• Enable MFA Delete to prevent accidental or intentional deletion • Enable SSE-S3 to encrypt S3 bucket contents • Restrictive S3 policies including personnel with access to logs	Apply and test restrictions Enable MFA and encryption	IAM Admin	2025-08-20	In Progress
POAM 08	Privileged admin actions not tied to individual identities	AU-10	• Create individual accounts for admin. • Create separate account with different permissions for privileged and no-privileged actions • Enforce MFA	Account set up Assign permissions Enable MFA Remove shared credentials	IAM Admin	2025-09-05	Open
POAM 09	No formal security awareness	AT-2	• Develop and roll out security awareness	Identify gaps in existing training plan	HR Lead Security Lead	2025-09-25	Planned

	training for staff		training including PII handling	Update training material Deliver sessions Track attendance Track understanding through tests	Privacy Officer		
POAM 10	Risk register is outdated	RA-3	• Update the risk register to include newly identified risks and show status of mitigated risk	Update and approve documentation	Risk Officer Security Lead	2025-10-10	Ongoing
POAM 11	Identified vulnerabilities not closed within prescribed timeframe	RA-5	• Create plan to close vulnerabilities on time to reduce risk of exploitation by threat actors	Create, document, test and implement patch plan	Risk Officer DevOps Security Engineer Application Security Analyst	2025-09-30	Ongoing
POAM 12	Delayed patching of non-critical servers beyond policy timelines	SI-2	• Enforce patch timelines with AWS Systems Manager Patch Manager automation	Configure, test and deploy patch rules	Systems Admin	2025-09-18	Ongoing
POAM 13	GuardDuty alerts not integrated into centralized SIEM	SI-4	• Integrate GuardDuty with AWS OpenSearch or third-party SIEM for real-time alerts	Design, correlate, parse, test and deploy logs	SOC Analyst Security Engineer	2025-09-08	Open

6. Authorize the System

A separate document with the ATO letter will accompany this document