SCRUM 5

FONTY’s ICT | S3 CS

Risk Analysis Report

Risk Management

Content

[Security Management Analysis Report 2](#_Toc184387143)

[1. Risk Assessment 2](#_Toc184387144)

[1.1 Asset Identification 2](#_Toc184387145)

[1.2 Threat Identification 2](#_Toc184387146)

[1.3 Vulnerabilities 2](#_Toc184387147)

[1.4 Impact and Likelihood Assessment 3](#_Toc184387148)

[2. Security Controls and Measures 3](#_Toc184387149)

[2.1 Access Control 3](#_Toc184387150)

[2.2 Data Protection 3](#_Toc184387151)

[2.3 Network Security 3](#_Toc184387152)

[2.4 Monitoring and Logging 3](#_Toc184387153)

[2.5 Incident Response Plan 3](#_Toc184387154)

[3. Compliance and Legal Considerations 4](#_Toc184387155)

[3.1 Regulatory Requirements 4](#_Toc184387156)

[3.2 Data Privacy 4](#_Toc184387157)

[4. Security Awareness and Training 4](#_Toc184387158)

[4.1 Employee Training 4](#_Toc184387159)

[4.2 Policy Enforcement 4](#_Toc184387160)

[5. Threat Intelligence and Vulnerability Management 4](#_Toc184387161)

[5.1 Threat Intelligence 4](#_Toc184387162)

[5.2 Vulnerability Management 4](#_Toc184387163)

[6. Incident Management and Response 5](#_Toc184387164)

[6.1 Incident Response Plan 5](#_Toc184387165)

[7. Business Continuity and Disaster Recovery 5](#_Toc184387166)

[7.1 Data Backup and Recovery 5](#_Toc184387167)

[7.2 Disaster Recovery Plan 5](#_Toc184387168)

[8. Security Metrics and Performance Evaluation 5](#_Toc184387169)

[8.1 Key Performance Indicators (KPIs) 5](#_Toc184387170)

[8.2 Audit Logs and Reports 5](#_Toc184387171)

[9. Recommendations and Action Plan 5](#_Toc184387172)

[Immediate Actions 5](#_Toc184387173)

[Long-Term Improvements 6](#_Toc184387174)

[Security Roadmap (Extended time) 6](#_Toc184387175)

# Security Management Analysis Report

**Summary**

This Security Management Analysis Report provides an evaluation of the security posture for the AWS infrastructure supporting the current project. The primary objective is to assess the effectiveness of existing security controls, identify potential risks, and offer actionable recommendations for improvement. Given the scale of the project, which is limited to a small school-related use case, this analysis focuses on core security aspects that will provide adequate protection without excessive cost.

This report outlines the risks, security measures, compliance considerations, and training needs for the business. Based on the findings, several improvements are recommended, particularly in areas like user access control, incident response, and ongoing monitoring to ensure data and systems are adequately protected.

Key assets like EC2 instances, S3 buckets, RDS databases, and IAM roles are at risk from threats such as external attacks, insider threats, data breaches, and DoS. Vulnerabilities include outdated software, weak access controls, and lack of encryption. The likelihood of these risks is moderate, with severe impact if sensitive data is exposed.

## 1. Risk Assessment

### 1.1 Asset Identification

The following critical assets were identified within the AWS environment for the project.

* **EC2 Instances** - Running the core applications and services.
* **S3 Buckets** - Storing sensitive project data, including backup files and project deliverables.
* **RDS Database** - Hosting project data and configuration settings.
* **IAM Roles and Policies** - Managing access controls for AWS resources.

### 1.2 Threat Identification

Key threats to the environment include the following.

* **External Attacks** - Potential threats from malicious actors attempting to exploit open ports, weak configurations, or vulnerabilities.
* **Insider Threats** - Risks associated with current or former users misusing their access rights.
* **Data Breaches** - Potential exposure of sensitive data stored in S3 buckets, EC2 instances, or databases.
* **Denial of Service (DoS)** - Possible risk of service downtime or disruption.

### 1.3 Vulnerabilities

Identified vulnerabilities include the following.

* **Outdated Software** - Some instances and services may be running older versions of software without the latest patches.
* **Weak Access Control** - Possible misuse of overly permissive IAM roles or missing multi-factor authentication (MFA) for certain users.
* **Lack of Encryption** - Inadequate encryption for sensitive data at rest or in transit.

### 1.4 Impact and Likelihood Assessment

The likelihood of threats such as data breaches or external attacks is moderate, given that some AWS resources may lack sufficient access controls or encryption. The impact of such incidents could be severe, particularly if sensitive project data is exposed. Based on history, that keys that are exposed will guide unauthorized users to the AWS dashboard. Due to requirements for the IAM users, they do require more reign power, making the security of the accounts more dire.

## 2. Security Controls and Measures

### 2.1 Access Control

* **Current State** - IAM roles are configured to control user access, but some users still have overly broad permissions. MFA is not enforced on all accounts.
* **Recommendation** - Implement the principle of least privilege for IAM policies, ensuring that users only have access to the resources they need. Enforce MFA across all accounts, particularly for privileged users.

### 2.2 Data Protection

* **Current State** - Some sensitive data in S3 and RDS are not encrypted at rest.
* **Recommendation** - Enable encryption for all data at rest and in transit, using AWS KMS (Key Management Service) for RDS and S3 encryption. Additionally, consider implementing encryption for backups.

### 2.3 Network Security

* **Current State** - VPC (Virtual Private Cloud) is configured with basic security groups and NACLs (Network Access Control Lists). However, there is room for improvement in restricting access to certain resources.
* **Recommendation** - Tighten security group rules to limit access based on IP addresses and services that truly need it. Consider setting up a Web Application Firewall (also known as WAF) for EC2 instances exposed to the internet.

### 2.4 Monitoring and Logging

* **Current State** - CloudTrail is enabled to monitor API calls and events, but logging is not consistently enabled for all services.
* **Recommendation** - Ensure CloudTrail is configured to log events across all regions. Enable **CloudWatch Logs** for detailed logging on EC2 instances and Lambda functions to monitor system health and suspicious activities.

### 2.5 Incident Response Plan

* **Current State** - There is no formal incident response plan in place.
* **Recommendation** - Develop and implement an incident response plan that includes processes for identifying, containing, and remediating security incidents. This plan should also include procedures for post-incident analysis.

## 3. Compliance and Legal Considerations

### 3.1 Regulatory Requirements

* **Current State** - The project does not directly fall under any specific industry regulations such as HIPAA or PCI-DSS but must comply with data privacy laws, especially if personal data is stored or processed.
* **Recommendation** - Ensure that all personally identifiable information (PII) is handled in accordance with General Data Protection Regulation (GDPR) or any other relevant local laws. This includes the implementation of encryption and access controls for sensitive data.

### 3.2 Data Privacy

* **Current State** - Sensitive data is stored on AWS services without explicit mention of encryption or access management.
* **Recommendation** - Follow best practices for data privacy, ensuring that sensitive information is encrypted and that access is logged and restricted to authorized users.

## 4. Security Awareness and Training

### 4.1 Employee Training

* **Current State** - No formal security awareness training has been conducted for users accessing the AWS environment.
* **Recommendation** - Implement regular security training sessions for all employees, covering key topics such as phishing, password security, and safe internet practices. This includes adding MFA onto your given account before gathering personal identifiable information (PII) or working

### 4.2 Policy Enforcement

* **Current State** - Employees may not fully adhere to security policies like password complexity and data handling procedures.
* **Recommendation** - Enforce security policies through automated tools (e.g., IAM policy checks) and ensure all employees are trained on security best practices.

## 5. Threat Intelligence and Vulnerability Management

### 5.1 Threat Intelligence

* **Current State** - No active threat intelligence program is in place.
* **Recommendation** - Subscribe to threat intelligence feeds or use AWS services like GuardDuty to gain insights into potential security threats. This could show important to keep up to date to the newest security threats.

### 5.2 Vulnerability Management

* **Current State** - Periodic vulnerability scanning is not implemented.
* **Recommendation** - Regularly perform vulnerability assessments using tools like AWS Inspector and schedule penetration testing to uncover potential weaknesses.

## 6. Incident Management and Response

### 6.1 Incident Response Plan

* **Current State** - No formalized incident response procedures.
* **Recommendation** - Develop a documented incident response plan, outlining roles, procedures, and tools for detecting, responding to, and recovering from security incidents.

## 7. Business Continuity and Disaster Recovery

### 7.1 Data Backup and Recovery

* **Current State** - Backups are automatically made with a 35 day retention due to longtivity of the project. Service used is AWS Backup.
* **Recommendation** - The daily backup is for critical data stored in S3 and RDS, to ensure that these backups are redundant, they should be encrypted and stored in a geographically separate region for redundancy.

### 7.2 Disaster Recovery Plan

* **Current State** - No formal disaster recovery plan in place.
* **Recommendation** - Develop a disaster recovery plan that includes detailed steps for restoring service and data after an outage or disaster. This plan should cover both internal resources and third-party services like AWS.

## 8. Security Metrics and Performance Evaluation

### 8.1 Key Performance Indicators (KPIs)

**Recommendation** - Establish KPIs to measure the effectiveness of security controls. These could include the following.

* + **Number of security incidents** detected.
  + **Time to detect and respond** to incidents.
  + **Percentage of systems with up-to-date patches**.

### 8.2 Audit Logs and Reports

* **Current State** - Audit logs are captured but not systematically reviewed.
* **Recommendation** - Set up an automated review process for audit logs and security reports, using tools like CloudWatch Logs Insights for better visibility.

## 9. Recommendations and Action Plan

### Immediate Actions

* Enable MFA for all AWS accounts.
* Implement encryption for data stored in S3 and RDS.
* Review and tighten IAM permissions to follow the least privilege principle.
* Develop and document an incident response plan.

### Long-Term Improvements

* Regularly conduct vulnerability assessments and penetration testing.
* Implement automated backups and disaster recovery procedures.
* Establish a formal security awareness training program for all employees.

### Security Roadmap (Extended time)

* **Next month** - Focus on improving IAM security, enforcing MFA, and implementing encryption for all sensitive data. Conduct regular security audits and establish a vulnerability management process.
* **Next 6 months** - Develop a comprehensive disaster recovery plan and invest in security monitoring tools such as AWS GuardDuty.

**Conclusion**

This analysis highlights the critical security risks faced by the AWS infrastructure and provides actionable recommendations to mitigate those risks. By addressing the identified gaps in access control, data protection, incident response, and compliance, the organization can significantly improve its security posture and protect its data and systems from potential threats.

Due this being a small scale project, does not take away from the security risks we are currently facing in our infrastructure. This document is supposed to give a insight on improvements that can be made.

Addressing identified gaps in access control, data protection, and incident response will improve security posture and reduce risks, even for a small-scale project.