PT 1: Project Proposal

Jamal Rizki

Improving Nebula Systems Amazon S3 Security and Availability

A1. Security Problem and Description

Nebula Systems recently migrated from an on-premise environment to a cloud solution through Amazon Web Services. The business currently relies heavily on Amazon Simple Storage Service (S3) to store business data. During a recent review, a key S3 bucket was found to have broad access permissions and the controls in place to protect the bucket are considered weak. If not remediated, these flaws can lead to unauthorized access, data exposure, data exfiltration, and reduced availability.

The importance of this problem is that it directly relates to the day-to-day business operations of the organization. Because Nebula Systems handles data in a regulated environment, data confidentiality, availability, and integrity are expected.

The current environment includes S3 for data storage, AWS IAM for user permissions, and CloudFront to globally distribute content. Any failure in this configuration can greatly impact the business. This impact may

occur from a regulatory perspective, a business process disruption, or a data loss or breach event.

A2. Problem Documentation

Industry frameworks and best practices demonstrate that S3 misconfigurations require remediation. According to AWS Security best practices for Amazon S3, access controls for S3 buckets should follow the principles of least-privilege (Amazon Web Services, 2023).

Regulatory requirements for the organization include:

PCI DSS Requirement 7 – States that organizations should only access cardholder data on a need-to-know basis. (PCI Security Standards Council [PCI SSC], 2022, Requirement 7).

PCI DSS Requirement 3 – This requirement mandates that companies securely manage the storage of cardholder data (PCI SSC, 2022, Requirement 3).

GDPR - This regulation from the European Union requires that organizations apply appropriate technical measures, including access

controls, to protect the personal data of subjects within the European Union (European Union, 2016).

NIST – The NIST framework recommends securely controlling access and implementing strong identity management to protect systems. (National Institute of Standards and Technology [NIST], 2020).

A3. Root Causes

Overly Broad Access – Initially the permissions set during the migration from on-premise to cloud allowed for wider access than was intended.

Encryption – There is currently no encryption set at either a bucket level or object level.

Availability – There is currently no redundancy measures in place. This could impact availability should an event occur.

Lack of System Hardening – During the migration process standard hardening processes were not implemented. Guidelines by PCI DSS, NIST, GDPR and AWS were not utilized.

B. Stakeholders

Business leadership – Business leadership plays a critical role in this project their implementation involvement involves owning the risk and resources, while also providing approval and direction for the project. The security problem directly impacts business leadership through data exposure, disruption of operations, and regulatory or and financial issues that directly affect the organization. Business leadership has a significant influence of stakeholders on project as their approval determines scope, priority, funding and success of the project.

IT Security Team – The security team is responsible for the technical requirements of the project. Their implementation involvement includes defining the requirements, aligning the posture with PCI DSS, GDPR and NIST standards to ensure the configuration meets these requirements. The security problem impacts this team because misconfigurations can lead to data exfiltration, unauthorized access, and compliance issues. The IT Security Team influences the project by defining and implementing the technical controls and system design

Legal and Compliance Teams – The Legal and Compliance Teams provide regulatory oversight throughout the project. Their implementation involvement includes documenting, reviewing, and monitoring the regulatory requirements and the organization's compliance to them. The security problem impacts these teams because misconfigurations can lead to fines, penalties, and failed audits. The Legal and Compliance Teams influence the project as they ensure all controls, and documentation align with regulatory and compliance requirements.

Infrastructure Team – The Infrastructure Team executes the technical implementation across the organization's systems. Their implementation involvement includes executing changes across overall organizational infrastructure. The security problem impacts this team because misconfigurations can result in system outages, added maintenance burdens, and an unstable environment overall. The Infrastructure Team influences the project because the successful implementation requires the system functions correctly and meets performance and availability needs.

C. Historical Data

Nebula Systems initially implemented the S3 bucket solution in early 2022. The organization migrated from an on-premise environment to a cloud-based one with Amazon Web Services. During this process, the access permissions were set to be very broad in nature to speed up the migration process and have minimal disruption to business processes. Records show that there is no bucket encryption, redundancy, or hardening that was applied during the migration. These security issues were uncovered during a configuration review of the AWS Management Console and S3 bucket IAM access management portal in late 2024. The review showed that the bucket had public read and write access permissions enabled, and it also lacked any type of encryption on the objects that were stored. An analysis of IAM brought to light 576 user profiles that had access to the bucket, indicating inadequate access controls. In January 2025, logs confirmed that encryption was still disabled. In May 2025, a DNS replication error occurred, leading to a large financial loss to the business and bringing to light the lack of redundancy and availability. In June 2025, a threat actor gained unauthorized access to the system and exfiltrated sensitive data. This was directly related to the lack of access controls and the absence of strong encryption. The current S3 configuration is not compliant with PCI DSS, GDPR, or NIST expectations.

D1. Project Methodologies

Nebula Systems will use PCI DSS, GDPR, NIST, and AWS best practices to guide the system hardening. These frameworks provide the requirements necessary to align with compliance. These frameworks provide robust measures to secure access controls, data, and system configurations. The approach will be to assess, apply, and then validate configurations.

D2. Project Launch

The following rollout phases will include a review of the current system configuration, the implementation of updated access, encryption, and availability controls. The rollout is considered complete when adequate access controls are implemented, encryption is enabled, and redundancy and availability are configured. From a compliance perspective, completion is when the configurations meet the requirements of PCI DSS, GDPR, and NIST.

D3. Project Implementation and Risks

Risks include incorrectly applying access controls, which may block legitimate users; this may cause unintended disruptions to the business. There is a medium likelihood of this occurring given the complexity of IAM policy configurations. Errors in access control configurations could also lead to inadvertent access by nefarious parties, which could lead to cyberattacks, this has a low to medium likelihood due to the oversight from the security team. The incorrect implementation of encryption and availability could lead to data becoming inaccessible to both internal and external parties, his risk has a low likelihood of occurrence as encryption and availability configurations are well-documented.

E. Training

The training will be directed toward the technical teams, as they will be responsible for maintaining the configuration once implemented. The delivery method will be a short internal training session on the implementation, and this will also include reference materials the team can use if needed. The content of the training will include the applied changes

and the reasoning behind these changes, and it will also reference the regulatory necessity of the update. The duration will be 30 minutes of material and 15 minutes for questions and/or concerns.

F. Required Resources and Costs

Assessment phase – The resources to be used in this phase are the AWS Management Console, AWS Identity and Access Management portal, and AWS Simple Storage Service. As these are existing services the organization utilizes, there will be no additional costs associated.

Design Phase – This will be a review of internal policy documentation as well and will heavily involve Legal and Compliance teams. Documents to review will be the PCI DSS Payment Card Industry Data Security Standard: Requirements and Testing Procedures, version 4.0, Regulation (EU) 2016/679 (General Data Protection Regulation), NIST's Security and Privacy Controls for Information Systems and Organizations, and AWS's Security Best Practices for Amazon S3. There will be no additional costs in this phase.

Implementation phase – The resources used in this phase will be internal technical teams including the Infrastructure and Security teams.

The AWS Management Console, AWS Identity and Access Management portal, AWS Simple Storage Service, and Amazon CloudFront will be used in this phase. The costs associated will arise from Amazon CloudFront, where the current data transfer rate is the first 1 TB free, then $0.085 per GB (Amazon Web Services, 2025).

Validation Phase – This phase will utilize internal testing tools, reviews, and compliance documentation. As this phase uses existing resources, there is no additional cost.

Documentation phase – This phase will utilize internal documentation. There is no additional cost associated during this phase.

The largest investment in this project will be by internal staff members. Internal staff time is covered under existing operational costs.

G. Deliverables

The final deliverables will be an updated configuration to the Amazon S3 bucket, documentation detailing the changes applied, and a document showing the alignment with PCI DSS, GDPR, NIST, and AWS Best Practices.

Timeline/Milestones:

Assessment phase – The duration of this phase is set for 1 month. The resources to be used in this phase are the AWS Management Console, AWS Identity and Access Management portal, and AWS Simple Storage Service.

Start date: 01/01/2026 - End date: 02/01/2026

Design Phase – This phase is expected to take 1 month. This will involve the Legal and Compliance teams, and the documentation to be used will be PCI DSS Payment Card Industry Data Security Standard: Requirements and Testing Procedures, version 4.0, Regulation (EU) 2016/679 (General Data Protection Regulation), NIST's Security and Privacy Controls for Information Systems and Organizations, and AWS's Security Best Practices for Amazon S3.

Start date: 02/01/2026 - End date: 03/01/2026

Implementation phase – As this phase is more technical, the timeframe will be extended to 2 months. The resources used in this phase will be the AWS Management Console, AWS Identity and Access

Management portal, AWS Simple Storage Service, and Amazon CloudFront. The teams to be involved are the Infrastructure and Security teams.

Start date: 03/01/2026 - End date: 05/01/2026

Validation Phase – The validation phase is expected to take 1 month. It will involve all teams that participated in the project to confirm the successful configuration implementation. The resources that will be used are internal testing tools, reviews, and compliance documentation.

Start date: 05/01/2026 - End date: 06/01/2026

Documentation phase – This phase will take about two weeks, and it will involve the team members who contributed to the project. The work will use internal documentation and collaboration tools.

Start date: 06/01/2026 - End date: 07/14/2026

H1. Formative and Summative Test Plans

Formative testing – Testing will be performed during the entire implementation and rollout periods. This includes checking access on the

both the bucket and object level, confirming that IAM permissions conform to requirements, running encryption tests to verify the data's integrity, and making sure CloudFront is delivering content as expected. The tools to be used in this process will be the AWS Management Console, AWS S3, AWS IAM, and internal testing tools.

Summative Testing – After all configuration changes are complete, a final round of testing will confirm that the S3 bucket enforces least-privilege access, the encryption functions properly and as expected, CloudFront availability is stable, and the updated configuration aligns with PCI DSS, GDPR, and NIST requirements.

H2. Acceptance Criteria and KPI's

Minimal acceptance criteria – The minimum requirements for the project to be considered complete are that S3 access controls follow the principle of least privilege, bucket and object encryption are enabled on stored data, CloudFront is functioning as expected and distributing content effectively, and compliance is aligned with PCI DSS, GDPR, and NIST.

Key performance indicators – This includes the validation and testing of access controls, the automated encryption of items in storage, the successful retrieval of data, and the verification that compliance s being met.

H3. Test Case Justification

The test cases are validated because they address the initial concerns of Nebula Systems. This includes the misconfiguration of S3 bucket access controls, a lack of data encryption, and insufficient availability of data. The test cases address this problem by confirming that only authorized access is allowed, data that is stored is properly encrypted, the data has high availability globally, and regulatory compliance is achieved.

H4. Results Analysis

The results will be analyzed by comparing the updated configuration to its previous baseline. The new configuration will be compared to compliance requirements. Any failures during the testing phase will be

documented and reviewed by the relevant stakeholders. Stakeholders will also review all results to confirm that Nebula Systems' objectives are being met. This will include confirmation that the final configuration meets all technical and compliance expectations.

PT 2: Technology-Supported Security Solution

Jamal Rizki

Improving Nebula Systems Amazon S3 Security and Availability

A. Policies

After completing the AWS S3 configuration remediation, Nebula Systems created several new policies and documents to reflect the updated configuration and security requirements of the environment. These include an S3 Access Control Policy that defines least-privilege boundaries for all users and systems, an S3 Encryption Policy that requires encryption for all data stored in the bucket, and an Availability Standard that documents the use of CloudFront to support data availability. The organization also updated its existing documentation to account for the changes that were made during the remediation process.

A1. Decision-Making

The updated policies improve the cybersecurity decision-making process by establishing clear expectations for how access controls, encryption settings, and availability should be enforced within the organization's cloud environment. These changes allow Nebula Systems to

assess risk and evaluate changes using a standardized baseline rather than the inconsistent settings that existed previously.

B. Assurance Criteria

This solution promotes automation by enabling automatic encryption for the data stored in the S3 buckets, which reduces the need for manual configuration when uploading data. This configuration builds on the modernization of security that occurred when Nebula Systems initially moved to the cloud. By using cloud-native capabilities to apply least-privilege access and enable encryption, the organization now has a more robust and modern system. The organization decided to go with AWS as it is currently the largest cloud provider, and by using AWS S3, AWS IAM, and CloudFront, along with security frameworks such as PCI DSS (PCI Security Standards Council [PCI SSC], 2022), GDPR (European Union, 2016), and NIST (National Institute of Standards and Technology [NIST], 2020), Nebula Systems is implementing industry-standard tools and frameworks to protect its data.

C. Data Collection and CIA

Data collection is handled by enabling AWS logging, which keeps a record of who accesses the S3 bucket and to record the actions they take. These AWS logs provide a granular overview of access activity and help to confirm that the system is working as intended. The solution that was implemented centered around the core cybersecurity concept of confidentiality, integrity, and availability of data during its implementation. The confidentiality of data is achieved by enforcing the principles of least privilege and implementing access controls. The integrity of data is maintained through the use of encryption, which helps prevent unauthorized changes to the data that is stored in the system. The availability of data is achieved by implementing CloudFront, which distributes the content globally and helps ensure users have consistent access to resources.

D. Incident Mitigation

The configuration update assists with the mitigation of security incidents by preventing unauthorized access to sensitive data stored on the system. It also reduces the chance of the data being altered, this was

accomplished by enforcing encryption. If an incident were to occur, having clearer access boundaries makes it easier to identify unusual behavior and then respond appropriately. The AWS logs also provide a record of access activity, that would aid in an investigation should an incident occur.

E. Cybersecurity Plan

The updated configuration resulted in revised documentation that reflects the new access controls, encryption settings, and the availability configuration. This documentation outlines how the S3 bucket should be properly configured and also how it should be maintained moving forward. This documentation establishes guidance on how future reviews will be conducted. This updated documentation aligns with the PCI DSS, GDPR, and NIST requirements that were identified in the project plan.

E1. Regulatory Compliance

One of the main goals of the remediation was to meet the companies' regulatory requirements. The updated configuration addresses these requirements. PCI DSS Requirement 7 is addressed by using the principles

of least-privilege and access controls, that ensure only authorized personnel can access cardholder data (PCI Security Standards Council [PCI SSC], 2022, Requirement 7). PCI DSS Requirement 3 is met by enabling encryption to protect all stored data, including data both at rest and in transit (PCI SSC, 2022, Requirement 3). GDPR requirements are satisfied in the updated configuration by strengthening access controls, as this is required when handling data belonging to any EU subject (European Union, 2016). In addition, the changes made to access controls and encryption follow the guidance provided in the NIST framework (National Institute of Standards and Technology [NIST], 2020).

E2. Applications and Tools

During the project's documentation phase, internal documentation was created detailing the S3 bucket's configuration. The documentation includes information on the access control changes, the encryption settings and current requirements, and how the availability of data is set up and routed. The materials that were created were done so to provide a reference for maintaining the system.

F. Post-Implementation

The post-implementation environment shows the updated configuration across AWS S3, IAM, and CloudFront. The access permissions were updated to follow the principles of least privilege, encryption was setup to encrypt all stored data both at rest or in transit, and CloudFront has been configured to improve the availability of the organizations data. The documentation and configuration updates support these changes and provide details on how the system is now set up

F1. Improved Security

The remediation work that was done during this project improves Nebula Systems' security posture by fixing the overly broad access permissions, adding strong encryption to all stored data, and by setting up consistent availability by utilizing CloudFront (Amazon Web Services, 2023). The updated configuration now has defined configuration requirements, which in turn make it easier to mitigate and respond to security incidents should they occur. The organization's efficiency also improved because the availability of data is now more reliable.

F2. Data Analysis

After the configuration updates, the access logs show that the correct access permissions and encryption are being applied and are working as anticipated. This improved access control and encryption means the business can maintain compliance with PCI DSS, GDPR, and NIST, and prevent security incidents that could disrupt business operations.

F3. Evaluation Plan

The summative testing was successful in verifying that the access controls meet least-privilege requirements. The testing also confirmed that encryption was enabled, and the availability of data had been remediated. The testing also confirmed that compliance with PCI DSS, GDPR, and NIST was met. During the testing phase there was some confusion surrounding IAM permissions for several departments, but this was clarified by business leadership and successfully applied.

F4. Post-Implementation Risks

Potential issues that could arise post-implementation are configuration drift and unauthorized modifications to access controls. Configuration drift has a medium likelihood of occurring, as multiple teams own data and could unintentionally alter settings. This has a high impact because it negates the work done to secure the system. Unauthorized modifications have a low likelihood due to the remediation efforts recently completed, but the impact would be significant, as someone elevating privileges could make configuration changes that disrupt the business. These risks can be mitigated by conducting regular reviews, updating documentation, and updating configurations regularly.

F5. Stakeholder Needs

The solution that was implemented meets the needs of all stakeholders involved in the project. Business leadership required a reduction in organizational risk and assurance that sensitive company data would remain protected. By using least privilege access and encryption, the organization now benefits from reduced exposure to unauthorized access and data loss. The Security Team needed a configuration that aligned with

established frameworks, including PCI DSS, GDPR, NIST, and AWS best practices. The system hardening, access control policies, and encryption now align with these frameworks, and there is a clear and updated system configuration that addresses the vulnerabilities that were identified. The Legal and Compliance teams required the system to align with regulatory needs, particularly the protection of sensitive data. The updated configurations updated access controls, improved data availability, and strengthened encryption, brings the system into alignment with PCI DSS, GDPR, and NIST requirements. Nebula Systems now meets its regulatory obligations. Finally, the Infrastructure Team needed a stable and reliable storage configuration that would prevent outages and reduce maintenance burdens. This was supported by implementing CloudFront to improve system availability, remediating the broken access controls, and enabling encryption. This benefits the Infrastructure Team by providing an environment that functions in a more stable and predictable manner.

G. Maintenance Plan

Ongoing maintenance will involve reviewing the configuration to confirm that access policies, encryption settings, and availability remain in

alignment with internal documentation. The configuration and documentation should be updated to address any changes in PCI DSS, GDPR, or NIST regulations. It should also cover updates made by AWS so that the configuration stays up-to-date and compliant.

H. Artifacts

policies.md

```
// Users //
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "BasicUser",
        "Effect": "Allow",
        "Action": [
          "s3:GetObject",
          "s3:ListBucket"
        ],
        "Resource": [
          "arn:aws:s3:::nebula-systems",
          "arn:aws:s3:::nebula-systems/*"
        ]
      }
    ]
  }

// HR Department //
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "HR",
        "Effect": "Allow",
        "Action": [
          "s3:GetObject",
          "s3:ListBucket"
        ],
        "Resource": [
          "arn:aws:s3:::nebula-systems",
          "arn:aws:s3:::nebula-systems/*"
        ]
      }
    ]
  }
```

Figure 1 IAM Policies for Standard Users and HR Department

```
//  IT Department //
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "IT",
        "Effect": "Allow",
        "Action": [
          "s3:GetObject",
          "s3:PutObject",
          "s3:DeleteObject",
          "s3:ListBucket"
        ],
        "Resource": [
          "arn:aws:s3:::nebula-systems",
          "arn:aws:s3:::nebula-systems/*"
        ]
      }
    ]
  }
```

Figure 2 IAM Policy for IT Department

References

Amazon Web Services. (2023). *Security best practices for Amazon S3.* https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html

PCI Security Standards Council. (2022). *Payment Card Industry Data Security Standard: Requirements and testing procedures, version 4.0.* https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf

European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88.* https://eur-lex.europa.eu/eli/reg/2016/679/oj

National Institute of Standards and Technology. (2020). Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 80053, Revision 5). https://doi.org/10.6028/NIST.SP.80053r5

Amazon Web Services. (2025). *Amazon CloudFront pricing.* https://aws.amazon.com/cloudfront/pricing/