**KING’S OWN INSTITUTE\***

**Success in Higher Education**

# GROUP ASSIGNMENT COVERSHEET

Subject Code & Name: Lecturer’s/Tutor’s name:

ICT742 Cloud Privacy and Security T324

Dr. MD Monir Hossain

Assignment Title:

Group Development Project: Northgate Financial Bank

**Declaration**

(This declaration must be completed by all students in the group or the assignment will not be marked.)

We, the undersigned, certify the following:

* We have read and understood the *Student Academic Misconduct Policy*
* This assignment is our own work based on our personal study and or research.
* We have acknowledged all material and sources used in the preparation of this assignment including any material generated in the course of our employment.
* **The assignment has not previously been submitted for assessment in this or any other unit.**
* We have not copied in part or in whole or otherwise plagiarised the work of other students.
* We have read and understand the criteria used for assessment.
* The assignment is within the word and page limits specified in the unit outline.
* The use of any material in this assignment does not infringe the intellectual property / copyright of a third party.
* We understand that this assignment may undergo electronic detection for plagiarism, and an anonymous copy of the assignment may be retained on the database and used to make comparisons with other assignments in future.
* By completing this coversheet in full and submitting this assignment electronically, we are bound by the conditions of the KOI's *Student Academic Misconduct Policy* and the declaration on this coversheet.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Family Name | Given Name(s) | Student ID | Tutorial Code | Contribution Percentage | Signature |
| Student 1 | Austria | John Benny | 12301175 | LA/NCLA | 33.33% | J\_AUST |
| Student 2 | Dumo | Carl Jasper | 12203645 | LA/NCLA | 33.33% | C\_DUMO |
| Student 3 | Paulino | Lovely | 12301035 | LA/NCLA | 33.33% | L\_PAULINO |

**Assignment Receipt**

Subject Code & Name: ICT742 Cloud Privacy and Security T324

Lecturer’s/Tutor’s Name: Dr. MD Monir Hossain

Assignment Title:

Group Development Project: Northgate Financial Bank

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Family Name | Given Name(s) | Student ID | Tutorial/ Code | Signature |
| Student 1 | Austria | John Benny | 12301175 | LA/NCLA | J\_AUST |
| Student 2 | Dumo | Carl Jasper | 12203645 | LA/NCLA | C\_DUMO |
| Student 3 | Paulino | Lovely | 12301035 | LA/NCLA | L\_PAULINO |

GROUP ASSIGNMENT COVER SHEET \* AUSTRALIAN INSTITUTE OF BUSINESS AND MANAGEMENT PTY LTD PAGE **1** OF **1**

16 January 2023 CRICOS 03171A ABN: 72 132 629 979

# EXECUTIVE SUMMARY

Northgate Financial Bank (NGF) is a bank based in Sydney, Australia that manages highly sensitive information such as the customer’s account details, bank transactions and their personal identification. Due to high demands of information coming in the bank, NGF decided to migrate its data and applications to the cloud to improve efficiency, reliability and the scalability of managing data.

At the outset, this transition to cloud is faced with potential threats against its security systems. The challenges include data breaches, unauthorized access, compliance with regulations to GDPR, PCI DSS and SOX, insider threats and human errors in cloud configurations. As a solution, NGF sought a cloud security strategy that will use AWS services that will manage the encryption of sensitive data, monitoring the activities inside the cloud, and ensure access control.

This paper will outline the problems and security challenges faced by NGF and specify which AWS services are implemented to tackle the problems and security challenges. Additionally, it highlights the security and compliance by implementing the eight AWS services. Finally, conclusion, future work, and plans for extension are given to summarize the information provided in the paper.

**TABLE OF CONTENTS**

[GROUP ASSIGNMENT COVERSHEET 1](#_Toc188721604)

[EXECUTIVE SUMMARY 2](#_Toc188721610)

[TABLE OF CONTENTS 3](#_Toc188721611)

[LIST OF FIGURES 5](#_Toc188721612)

[LIST OF TABLES 6](#_Toc188721613)

[1.0. PROBLEM DESCRIPTION 7](#_Toc188721614)

[2.0. CLOUD SERVICES USED 9](#_Toc188721615)

[2.1. Networking and Infrastructure 9](#_Toc188721616)

[2.1.1. Amazon Virtual Private Cloud 9](#_Toc188721617)

[2.1.2. Amazon EC2 Virtual Machine 10](#_Toc188721618)

[2.2. Security and Privacy 10](#_Toc188721619)

[2.2.1. AWS Security Groups and Network ACL 10](#_Toc188721620)

[2.2.2. Identity and Access Management (IAM) 11](#_Toc188721621)

[2.2.3. AWS Key Management Service (KMS) 11](#_Toc188721622)

[2.2.4. AWS Firewall Manager 12](#_Toc188721623)

[2.3. Monitoring and Governance 13](#_Toc188721624)

[2.3.1. AWS CloudTrail 13](#_Toc188721625)

[2.4. Storage 13](#_Toc188721626)

[2.4.1. AWS S3 Bucket 13](#_Toc188721627)

[3.0. SECURITY AND PRIVACY CHALLENGES 15](#_Toc188721628)

[3.1. Data Breaches and Unauthorized Access 15](#_Toc188721629)

[3.2. Compliance and Regulatory Concerns 16](#_Toc188721630)

[3.3. Insider Threats and Misconfigurations 17](#_Toc188721631)

[4.0. DETAILED DESCRIPTION OF THE SECURITY SOLUTION USING AWS SERVICES 18](#_Toc188721632)

[4.1. Amazon Virtual Private Cloud 18](#_Toc188721633)

[4.2. Amazon EC2 Virtual Machine 19](#_Toc188721634)

[4.3. AWS Security Groups and Network ACL 20](#_Toc188721635)

[4.4. AWS S3 Bucket 22](#_Toc188721636)

[4.5. Identity and Access Management (IAM) 23](#_Toc188721637)

[4.6. AWS Key Management Service (KMS) 25](#_Toc188721638)

[4.7. AWS CloudTrail 26](#_Toc188721639)

[4.8. Amazon Firewall Manager 27](#_Toc188721640)

[4.9. Summary 28](#_Toc188721641)

[5.0. CONCLUSION 29](#_Toc188721642)

[5.1. Future Work 29](#_Toc188721643)

[5.2. Plans for Extension 30](#_Toc188721644)

[REFERENCES 32](#_Toc188721645)

# LIST OF FIGURES

[Figure 2‑1. Amazon VPC 9](#_Toc188721658)

[Figure 2‑2. Amazon EC2 10](#_Toc188721659)

[Figure 2‑3. AWS Security Group 10](#_Toc188721660)

[Figure 2‑4. Amazon Web Services 11](#_Toc188721661)

[Figure 2‑5. AWS KMS 11](#_Toc188721662)

[Figure 2‑6. AWS Firewall Manager 12](#_Toc188721663)

[Figure 2‑7. Amazon CloudTrail 13](#_Toc188721664)

[Figure 2‑8. Amazon S3 Bucket 13](#_Toc188721665)

[Figure 4‑1. NGF Virtual Private Cloud 18](#_Toc188721666)

[Figure 4‑2. NGF EC2 Virtual Machine 19](#_Toc188721667)

[Figure 4‑3. NGF Security Group 20](#_Toc188721668)

[Figure 4‑4. NGF Network ACL 21](#_Toc188721669)

[Figure 4‑5. NGF S3 Bucket 22](#_Toc188721670)

[Figure 4‑6. NGF Roles 23](#_Toc188721671)

[Figure 4‑7. NGF Users 24](#_Toc188721672)

[Figure 4‑8. NGF Key Management 25](#_Toc188721673)

[Figure 4‑9. NGF CloudTrail 26](#_Toc188721674)

[Figure 4‑10. NGF Firewall Security Policy 27](#_Toc188721675)

# LIST OF TABLES

[Table 3‑1. Causes of Data Breaches 15](#_Toc188721676)

[Table 3‑2. Compliance Requirements 16](#_Toc188721677)

[Table 4‑1. AWS Services Summary 28](#_Toc188721678)

# PROBLEM DESCRIPTION

Northgate Financial Bank manages highly sensitive customer information that includes customer’s account information, personal identification and bank transactions. As part of the bank’s strategic initiatives, they plan to eventually migrate all their data to the cloud. While this plan aims to achieve scalability, efficiency in operation and also cost effectiveness it will face massive security challenges and risks which are associated with cloud migration if NFC transitions from on premise data management to cloud based and will affect the data’s integrity, confidentiality and availability. Migrating these data which have sensitive information to the cloud makes it an attractive target for attackers and will therefore be vulnerable to security risks or data breaches such as:

1. Unauthorized access and data breaches - This could result in exposure of sensitive information of the customer to the malicious attackers. Cyber Attackers are known to be persistent and work sophistically using advanced techniques just to exploit vulnerabilities.
2. Compliance violations due to inadequate data protection - As a financial institution, it should follow all the data protection regulations and standards which includes the Payment Card Industry Data Security Standard (PCI DSS) and the General Data Protection Regulation (GDPR). If they fail to comply and implement adequate security measures it could lead to having penalties, reputational damage and the customer’s trust will also be broken.
3. Insider threats and human errors in cloud configurations - Insiders can compromise the security by mishandling or misconfiguration of the cloud resources whether they are acting maliciously or inadvertently. Also, human errors such as giving excessive permission to a person or failing to implement proper encryption will probably result in sensitive information being vulnerable to exploitation.

Given these risks, NFC requires a comprehensive and robust cloud solution that not only guarantees the highest levels of data security but also privacy. The financial institution requires a cloud solution that not only guarantees data security but also ensures privacy while complying with the standards such as PCI DSS and GDPR.

The solution the institution needs must address potential vulnerabilities, will enforce strong access controls, can provide advanced encryption for data both at rest and in transit and can also support real time monitoring to detect and mitigate threats proactively.

# CLOUD SERVICES USED

By utilizing the AWS services, Northgate Financial can greatly enhance its scalability and security, as well as compliance, while also benefiting from the cost-effective nature of the cloud platform. AWS provides Northgate Financial with a robust and flexible infrastructure that allows it to expand as business demands rise. With its advanced encryption, threat detection, and identity management features, AWS is a top-tier security solution that protects sensitive financial information from potential security threats.

## Networking and Infrastructure

### Amazon Virtual Private Cloud



Figure ‑. Amazon VPC

Amazon VPC is a type of VPN that serves as resembling the public internet for companies. By using cloud-based services, organizations can use it to limit access within their network and avoid security risks (Amazon Web Services, 2024).

### Amazon EC2 Virtual Machine



Figure ‑. Amazon EC2

By offering Amazon EC2, AWS provides companies with the ability to reduce expenses related in part to buying expensive hardware and operating systems through its web service. Amazon Web Services has developed a service that allows businesses to control the capacity of virtual servers, customize networking and security settings, and manage storage capacity (Amazon Web Services, 2024).

## Security and Privacy

### AWS Security Groups and Network ACL



Figure ‑. AWS Security Group

AWS resources are accessed from a VPC by security groups and network ACLs. Inbound and outbound traffic are managed by security groups at the instance level, while network ACLs operate at a VPC subnet level. In 2024, Amazon Web Services provided both at no charge (Amazon Web Services, 2024).

### Identity and Access Management (IAM)



Figure ‑. Amazon Web Services

AWS Identity and Access Management (IAM) is a web service that offers access control features, which allows companies to manage users and assign roles and responsibilities. This allows for user authentication and authorization to be managed in organization's systems (Amazon Web Services, 2024).

### AWS Key Management Service (KMS)



Figure ‑. AWS KMS

AWS Key Management Service (KMS) facilitates the generation and management of cryptographic keys for companies. To prevent unauthorized changes and safeguard data during transmission, these encrypted keys are utilized (Amazon Web Services, 2024).

### AWS Firewall Manager



Figure ‑. AWS Firewall Manager

AWS Firewall Manager is an integrated security management solution that allows for the centralized establishment and administration of firewall policies across multiple accounts and applications within AWS Organizations. (Amazon Web Services, 2024).

## Monitoring and Governance

### AWS CloudTrail



Figure ‑. Amazon CloudTrail

AWS CloudTrail provides services that help with operational auditing, risk management, governance and compliance for AWS accounts. By capturing events from user, role or AWS services, it also tracks activities by using the AWS Console, AWS Command Line Interface, and various AWS SDKs as well as APIs. (Amazon Web Services, 2024).

## Storage

### AWS S3 Bucket



Figure ‑. Amazon S3 Bucket

On the AWS Simple Storage Service (S3) platform, objects are stored in a storage resource called an Amazon S3 bucket. Objects are used to store data in S3 buckets, rather than using traditional file storage. Similar to file folders, buckets on Amazon S3 are functionally used for storage, retrieval, backup, and accessing objects. Every object is composed of three primary elements: the data content, a unique identifier, and an additional layer (TechTarget, April 2023).

# SECURITY AND PRIVACY CHALLENGES

## Data Breaches and Unauthorized Access

Data breaches and unauthorized access occur when sensitive data has been accessed, disclosed or stolen without proper authorization. If access control is weak and easy to access, the migration process of data exposes it with potential breaches.

Unauthorized access can occur due to compromised credentials, unprotected endpoints or sophisticated hacking attempts. These incidents can have severe consequences such as financial loss, reputational damage and compromise the user trust. To mitigate these risks, it is critical to implement robust access controls that restrict unauthorized personnel from accessing sensitive systems.

Causes of Data Breaches:



Table ‑. Causes of Data Breaches

## Compliance and Regulatory Concerns

Northgate Financial Bank operates within a heavily regulated industry, requiring strict adherence to various compliance requirements such as GDPR, PCI DSS and SOX.

Compliance Requirements:



Table ‑. Compliance Requirements

Non-compliance can result to legal penalties, reputational damage and financial losses. Maintaining data sovereignty which ensures that data remains within approved jurisdictions is another critical aspect of compliance that needs to be followed and strictly implemented.

Ensuring compliance requires the implementation of detailed audit trails that log all activities involving sensitive data. This includes access attempts, configuration changes, and data transfers. Regular compliance checks and reporting capabilities are necessary to demonstrate adherence to regulatory standards and maintain stakeholder trust.

## Insider Threats and Misconfigurations

Insider threats can come from malicious intent and unintended actions by employees working in the same organization. Those malicious individuals might exploit their access to sensitive systems for their personal or external benefit while the negligent insiders might unconsciously expose vulnerabilities through their careless actions such as having weak passwords and even sharing sensitive information to unauthorized person.

Vulnerabilities can also originate or come from misconfigurations such as the improper configuration of security groups, excessive permissions and unprotected APIs. To address these challenges, it will require security awareness among the employees or within the organization, automated configuration checks, and incident detection systems to quickly identify and remediate potential issues.

# DETAILED DESCRIPTION OF THE SECURITY SOLUTION USING AWS SERVICES

## Amazon Virtual Private Cloud

Challenges Addressed:

* Data Breaches and Unauthorized Access
* Insider Threats and Misconfigurations

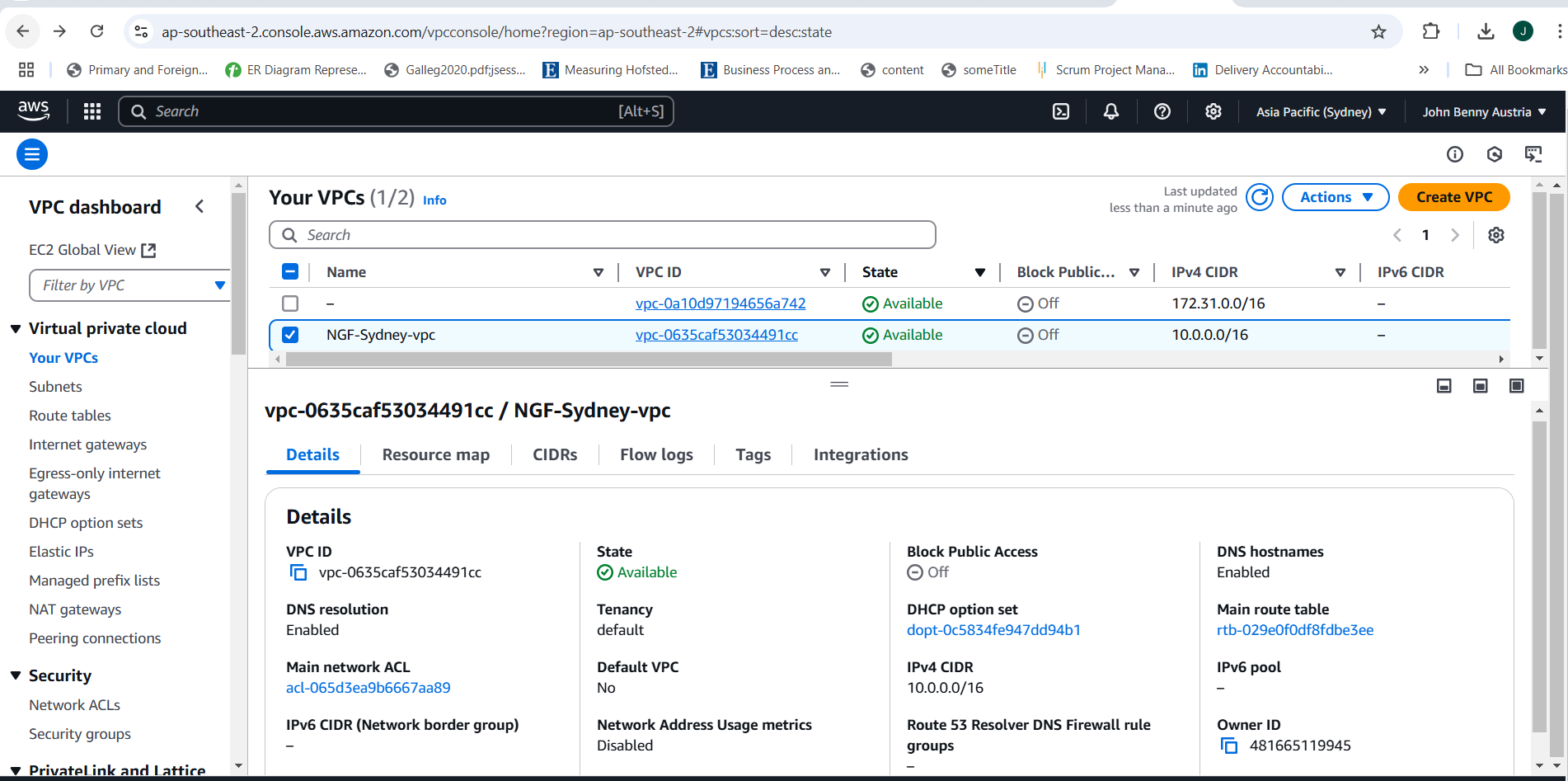


Figure ‑. NGF Virtual Private Cloud

To address the challenges in Northgate Financial Bank Cloud Service, Amazon VPC is deployed, as seen from Figure 4.0-1. Mane and Ainapure (2021) describe that “Private cloud computing incorporates numerous advantages of public cloud-like versatility, self-administration, and flexibility with extra control and customization.” The VPC reduces the exposures of attack by ensuring NGF’s sensitive systems such as databases are hosted in privacy subnets.

Amazon VPC uses NAT Gateways and Internet Gateways to control the internet access and minimizing lateral movements during an attack.

## Amazon EC2 Virtual Machine

Challenges Addressed:

* Data Breaches and Unauthorized Access
* Insider Threats and Misconfigurations

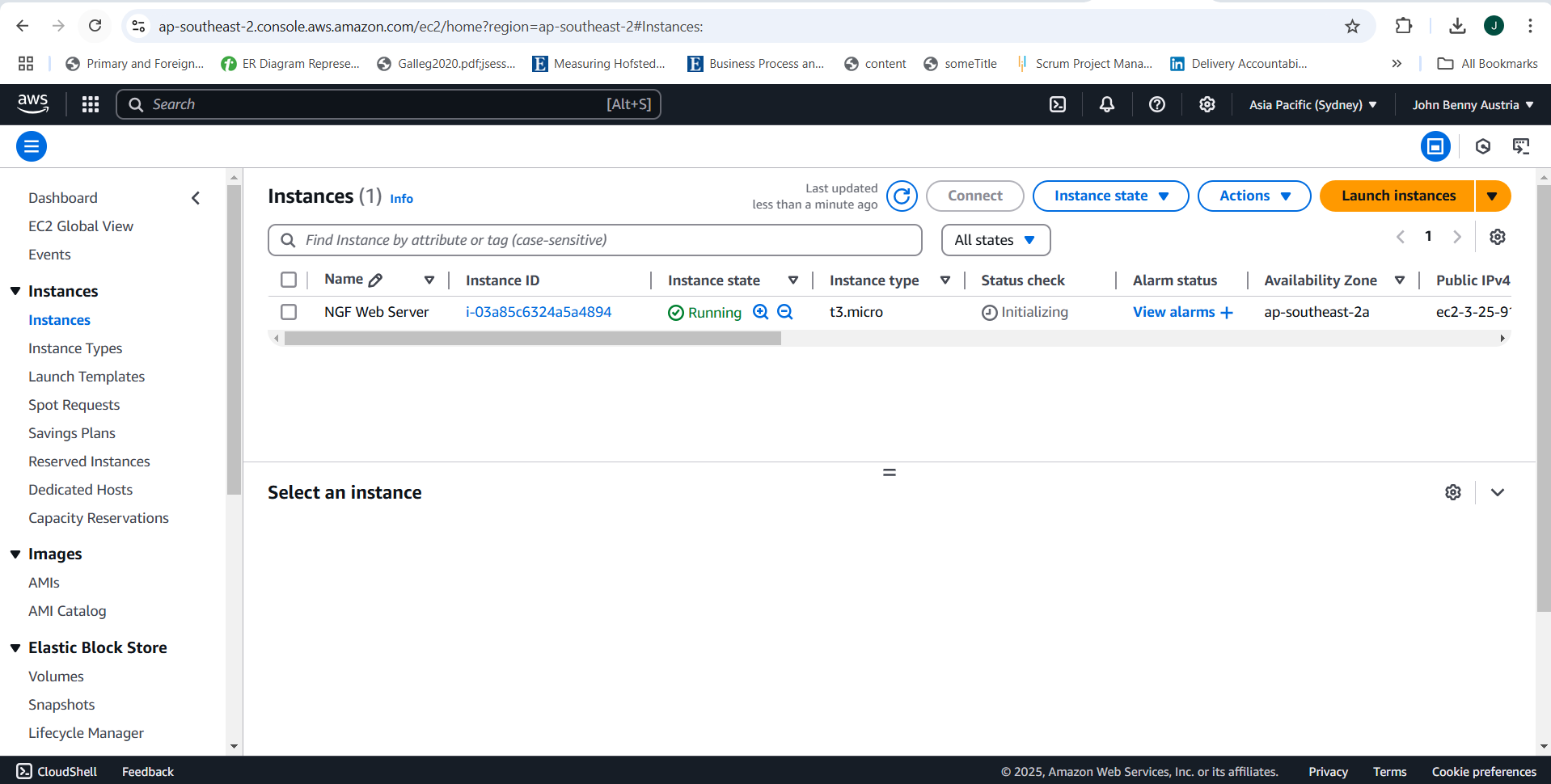


Figure ‑. NGF EC2 Virtual Machine

As NGF bank computers are running on windows, an EC2 Microsoft Windows Server 2025 Base is deployed in the web server of NGF. Figure 4.0-2 shows that the instace type is y3-micro and is available in ap-southeast-2a as the bank is based in Sydney. With this EC2 instance, it ensures that sensitive network workloads will not be directly exposed to the internet. The EC2 instance also encrypts sensitive financial data stored on EBS volumes and only allows authorized IP addresses to EC2 instance with security groups.

EC2 instance is an on-demand service that deploys their applications and rent virtual services hourly. Depending on the dynamics of the website’s traffic of NGF, users such as the admin can easily decrease or decrease the number of EC2 instances. As an illustration, AWS EC2 instances have the ability to eliminate any need for additional hardware and software expenses and maintenance (Choudhary, Verma and Rai, 2021).

## AWS Security Groups and Network ACL

Challenges Addressed:

* Data Breaches and Unauthorized Access
* Insider Threats and Misconfigurations

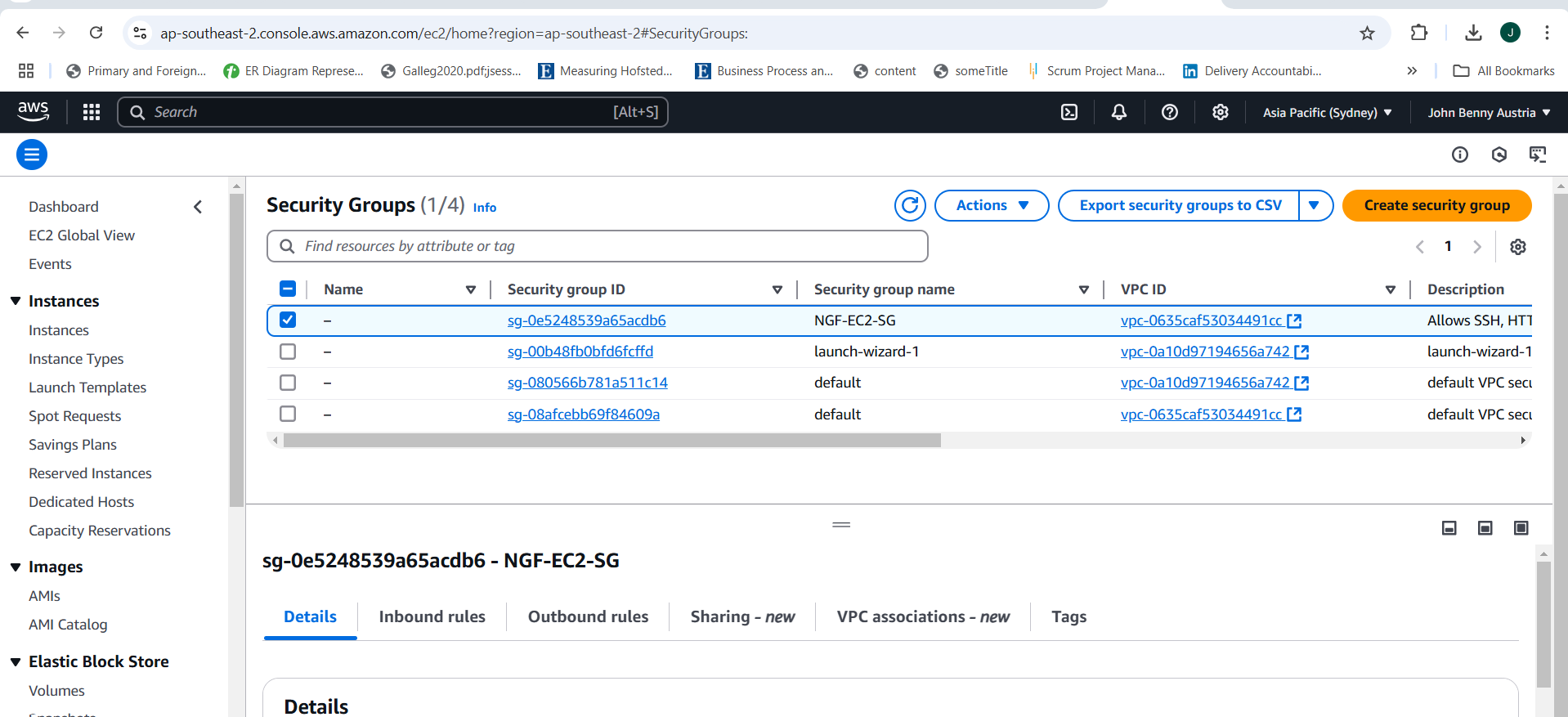


Figure ‑. NGF Security Group

NGF Security Group ensures that EC2 instances are protected through granular access control, meaning that it has specific inbound and outbound rules inside the system. Security groups control the traffic and acts as a virtual firewall and are stateful. instance. AWS (2024) describes that “the security group acts as a virtual firewall. The only traffic that reaches the instance is the traffic allowed by the security group rules.”

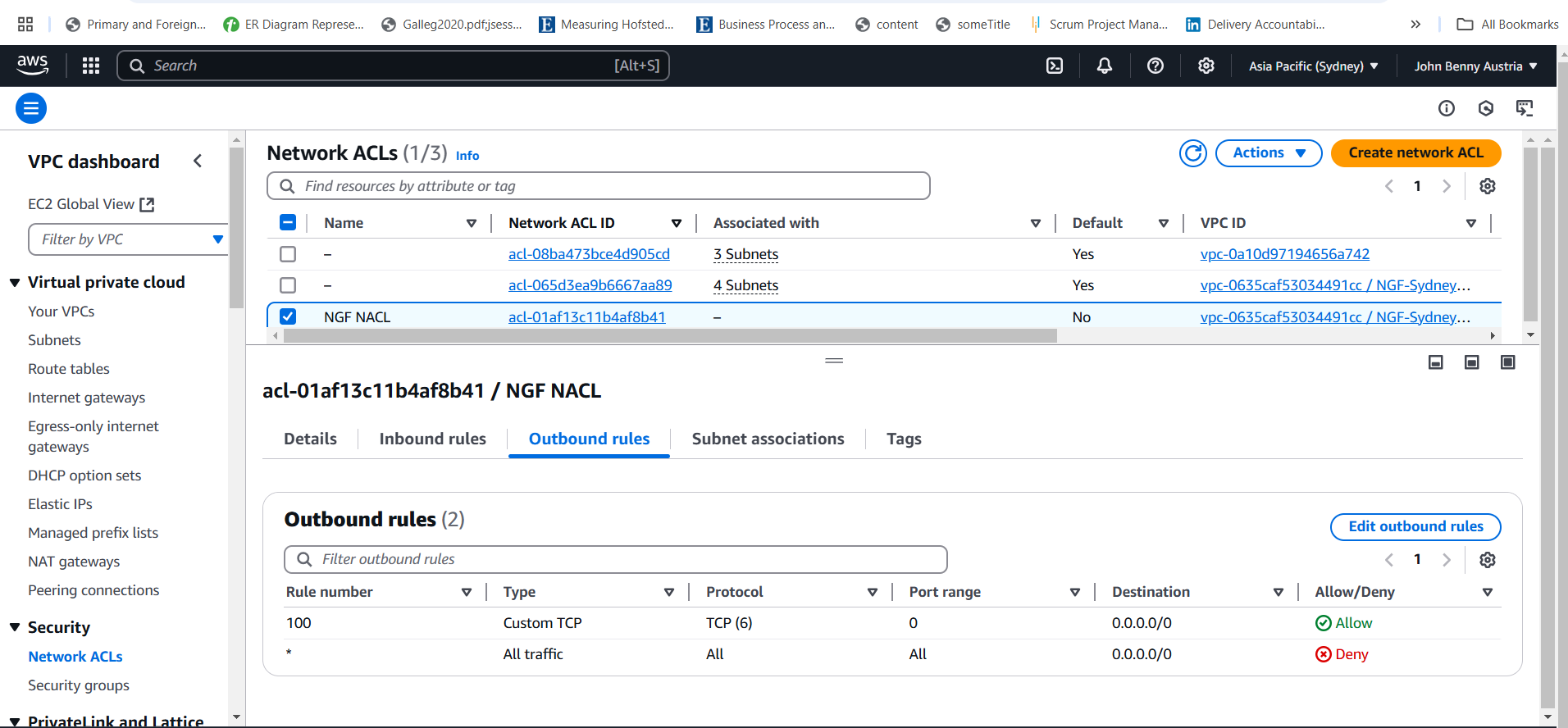


Figure ‑. NGF Network ACL

The Network ACL of NGF is connected to the NGF’s VPC. It has inbound rules from certain port ranges that specify which sources are allowed or denied in the system. This system also acts like a firewall for controlling traffic in and out of a subnet instead of an instance. Additionally, users can associate multiple subnets in a single network ACL, but on the other hand, a subnet can only be associated in one network ACL.

## AWS S3 Bucket

Challenges Addressed:

* Data Breaches and Unauthorized Access
* Compliance and Regulatory Concerns

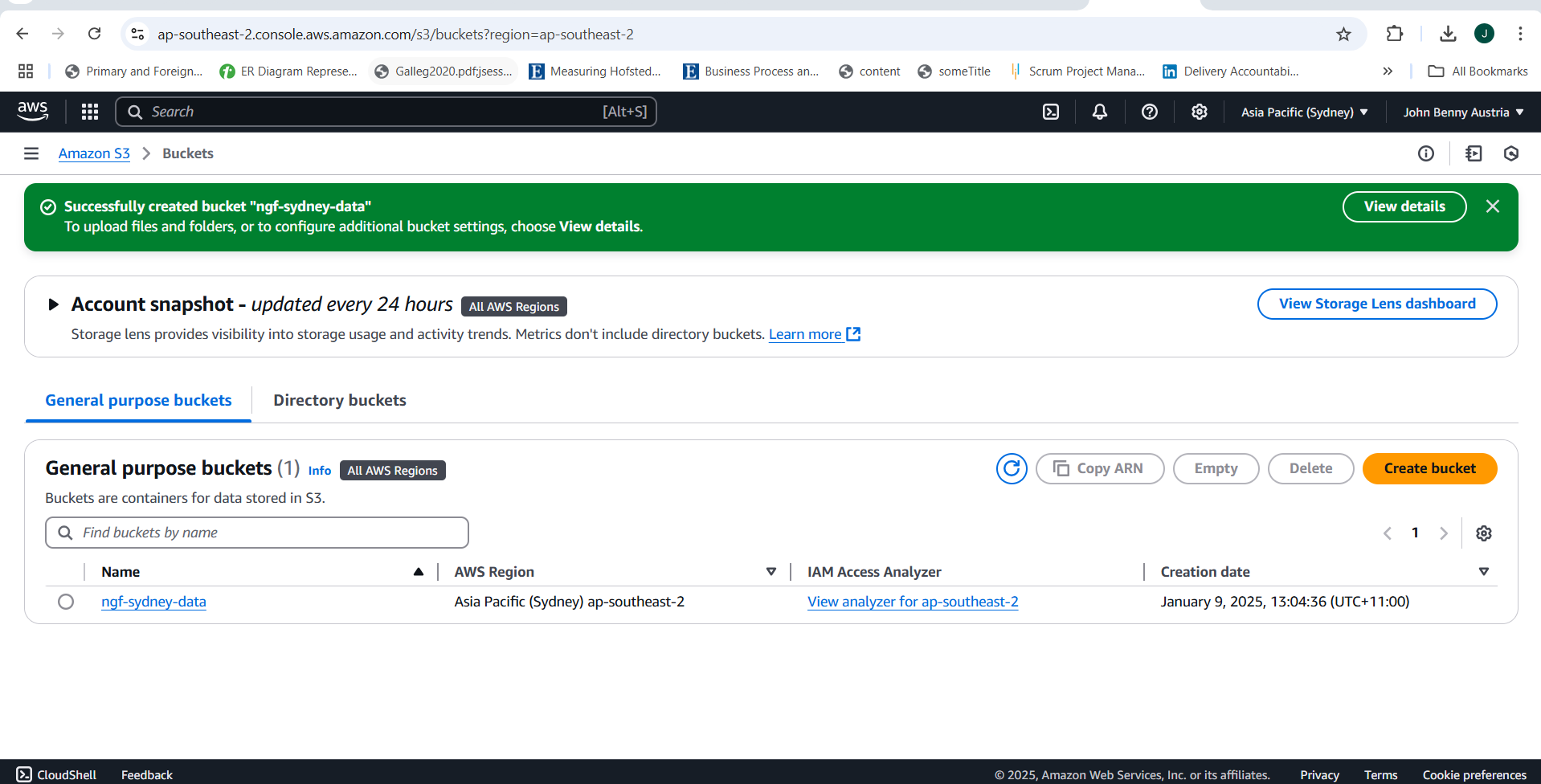


Figure ‑. NGF S3 Bucket

Juvonen (2023) states that “An Amazon S3 bucket is a public cloud storage resource available in Amazon Web Services (AWS) Simple Storage Service (S3) platform. It provides object-based storage, where data is stored inside S3 buckets in distinct units called objects instead of files.”

Since AWS S3 buckets supports Server-Side Encryption, NGF can store the transaction logs of the customers in an encrypted S3 bucket, ensuring that the transaction is only accessible by processing the EC2 instance. NGF’s bucket also complies with the local regulations of Sydney as NGF is based in Sydney region holding the data sovereignty.

## Identity and Access Management (IAM)

Challenges Addressed:

* Data Breaches and Unauthorized Access
* Insider Threats and Misconfigurations
* Compliance and Regulatory Concerns

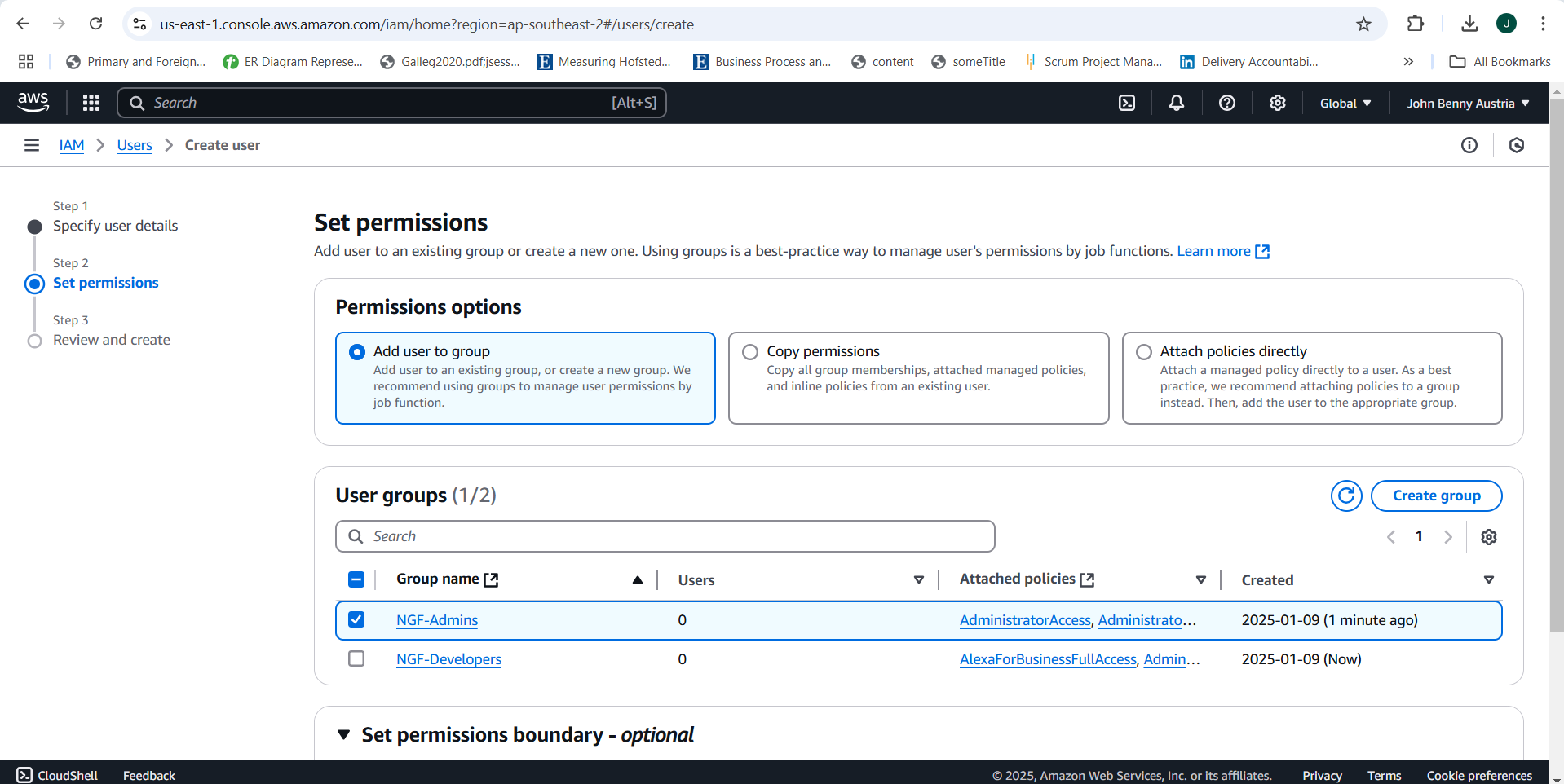


Figure ‑. NGF Roles

The roles assigned in NGF Identity and Access Management (IAM) are NGF-Admins which has full control over the resources and services and NGF-Developers which have limited access to the AWS services of NGF. NGF-Developers focuses on application and infrastructure management and can manage EC2 instances fully.

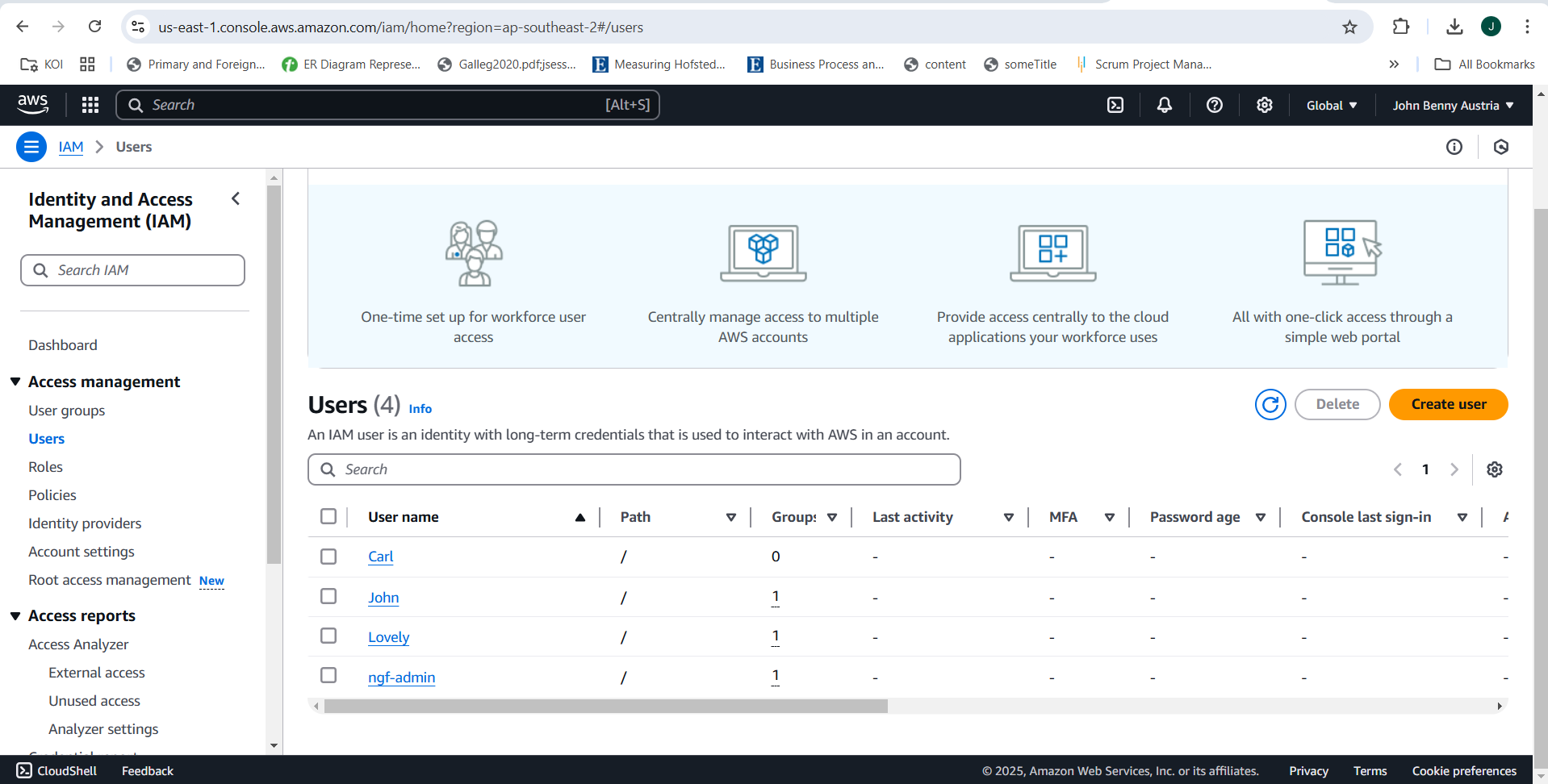


Figure ‑. NGF Users

As of the moment, only four users are created in IAM of NGF. John and ngf-admin belong to the NGF-Admins which have full access to AWS services, and manage all AWS resources, assigning permissions to each user and monitor the account activities of each user in NGF AWS service.

Lovely and Carl belong to NGF-Developers group which focus more on EC2 instance management. Although they have no full access to the AWS services, they can modify instance configurations and configure security groups and network ACL that are related to EC2.

Through IAM, specific services are only accessible to trusted and authorized users and applications, it will lessen the threats of insider threats, therefore increasing the security of AWS services used by NGF.

## AWS Key Management Service (KMS)

Challenges Addressed:

* Data Breaches and Unauthorized Access
* Compliance and Regulatory Concerns

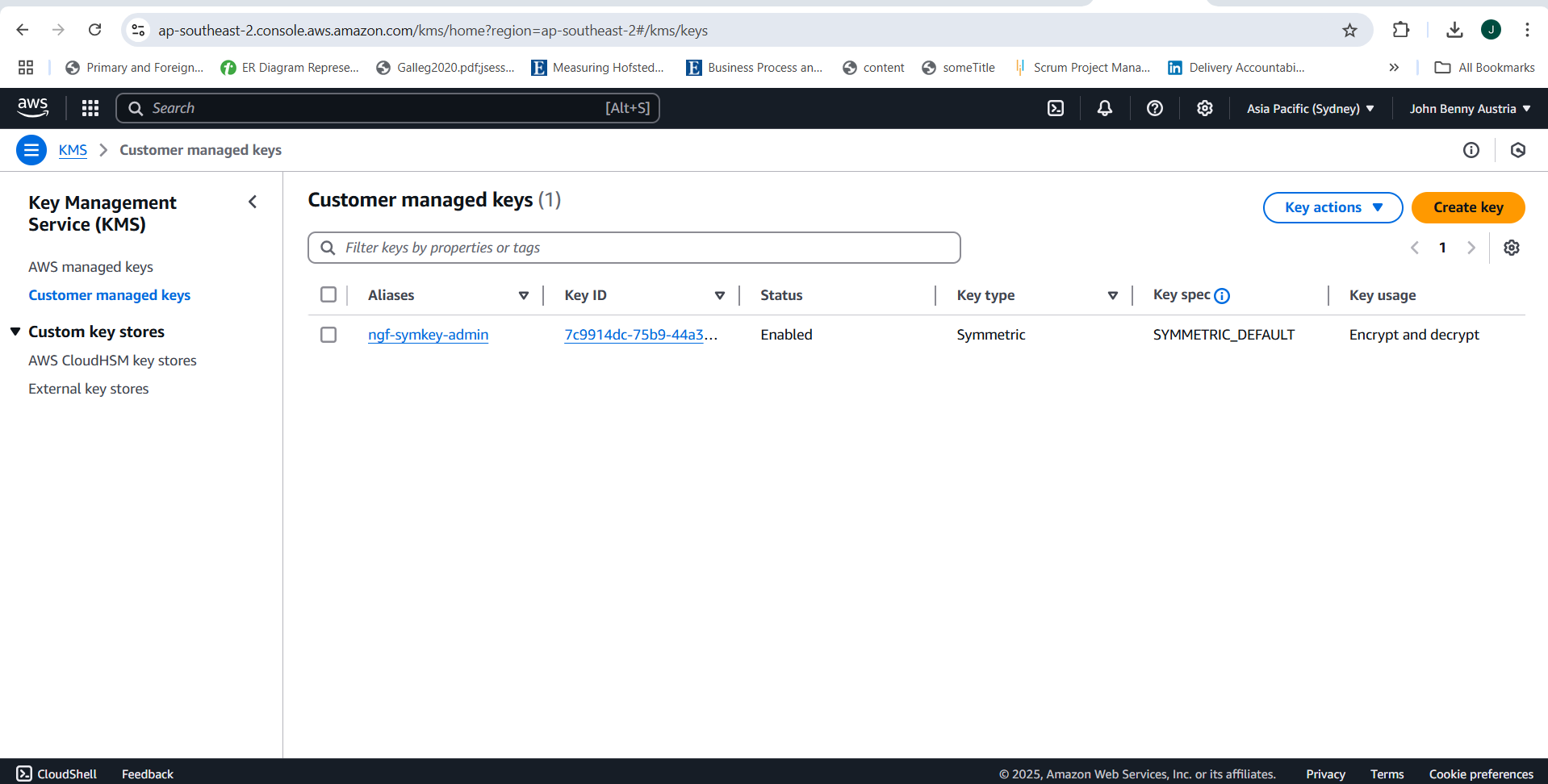


Figure ‑. NGF Key Management

Moore et al. (n.d.) declares that “AWS KMS allows customer to create, manage, rotate, and delete their customer-owned encryption keys. Each encryption key managed within KMS includes attached metadata that customers can view, such as the key ID, key spec, key usage, creation date, description (optional), key state, and key material.”

With AWS KMS, NGF Key management is centralized managing encryption keys for S3 and other AWS services that ensures data is encrypted while at transit or at rest. NGF Key management will also only authorized users such as John as described in IAM to manage and use the encryption keys. The keys in NGF are also periodically rotated to reduce the risk of outdated keys being exploited by hackers.

## AWS CloudTrail

Challenges Addressed:

* Data Breaches and Unauthorized Access
* Insider Threats and Misconfigurations
* Compliance and Regulatory Concerns

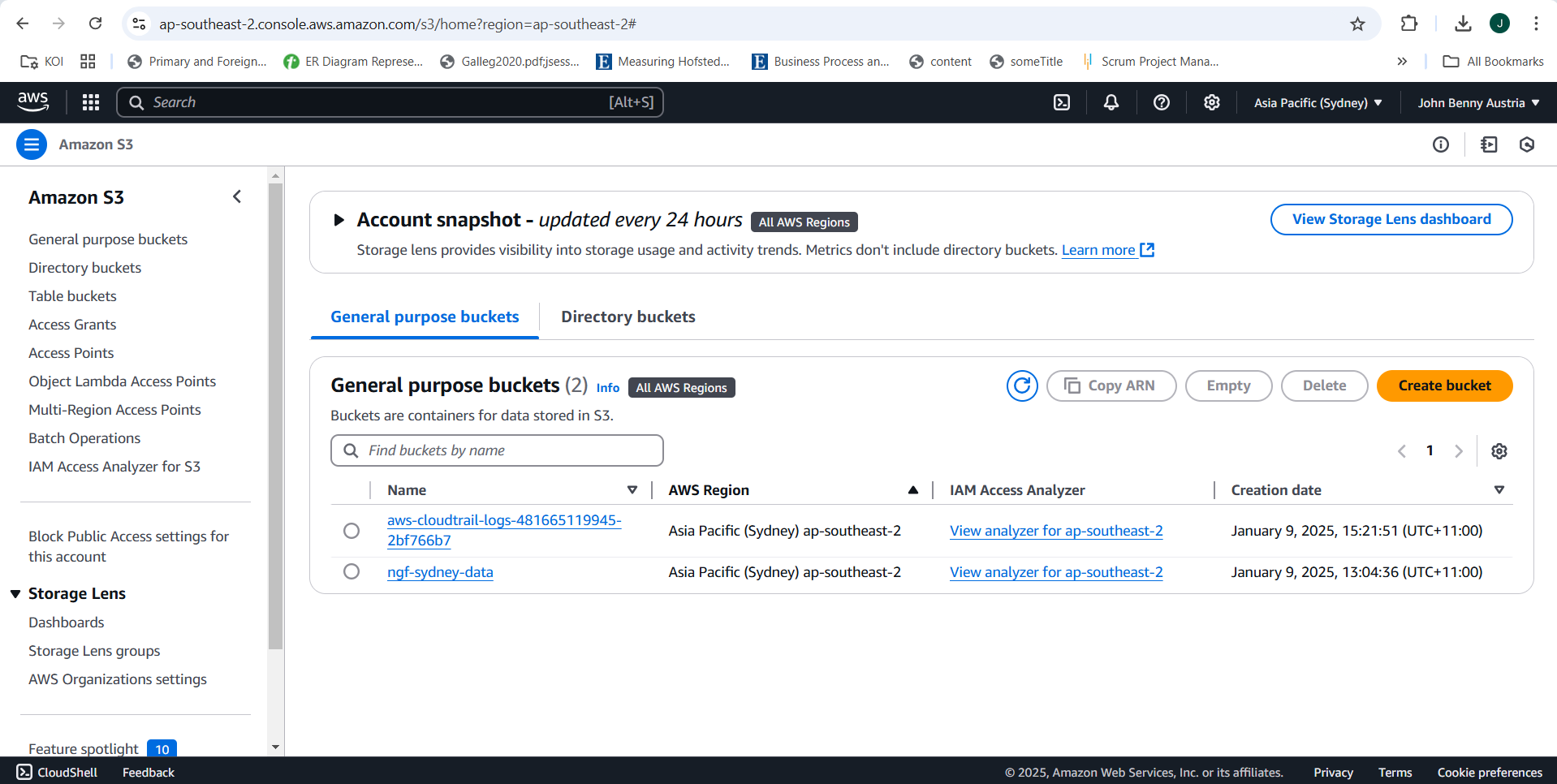


Figure ‑. NGF CloudTrail

Any changes made within an AWS service is traced through AWS CloudTrail as CloudTrail provides records of detailed logs for every API call and resources changes. Through analysis, NGF can automatically infer metadata attributes for each resource that will generate a comprehensive set of tags.

As NGF CloudTrail tracks changes and access to any sensitive resources, it will create a compliance report that will be sent to NGF’s bucket. This also ensures the compliance within the GDPR requirements.

## Amazon Firewall Manager

Challenges Addressed:

* Data Breaches and Unauthorized Access
* Insider Threats and Misconfigurations
* Compliance and Regulatory Concerns

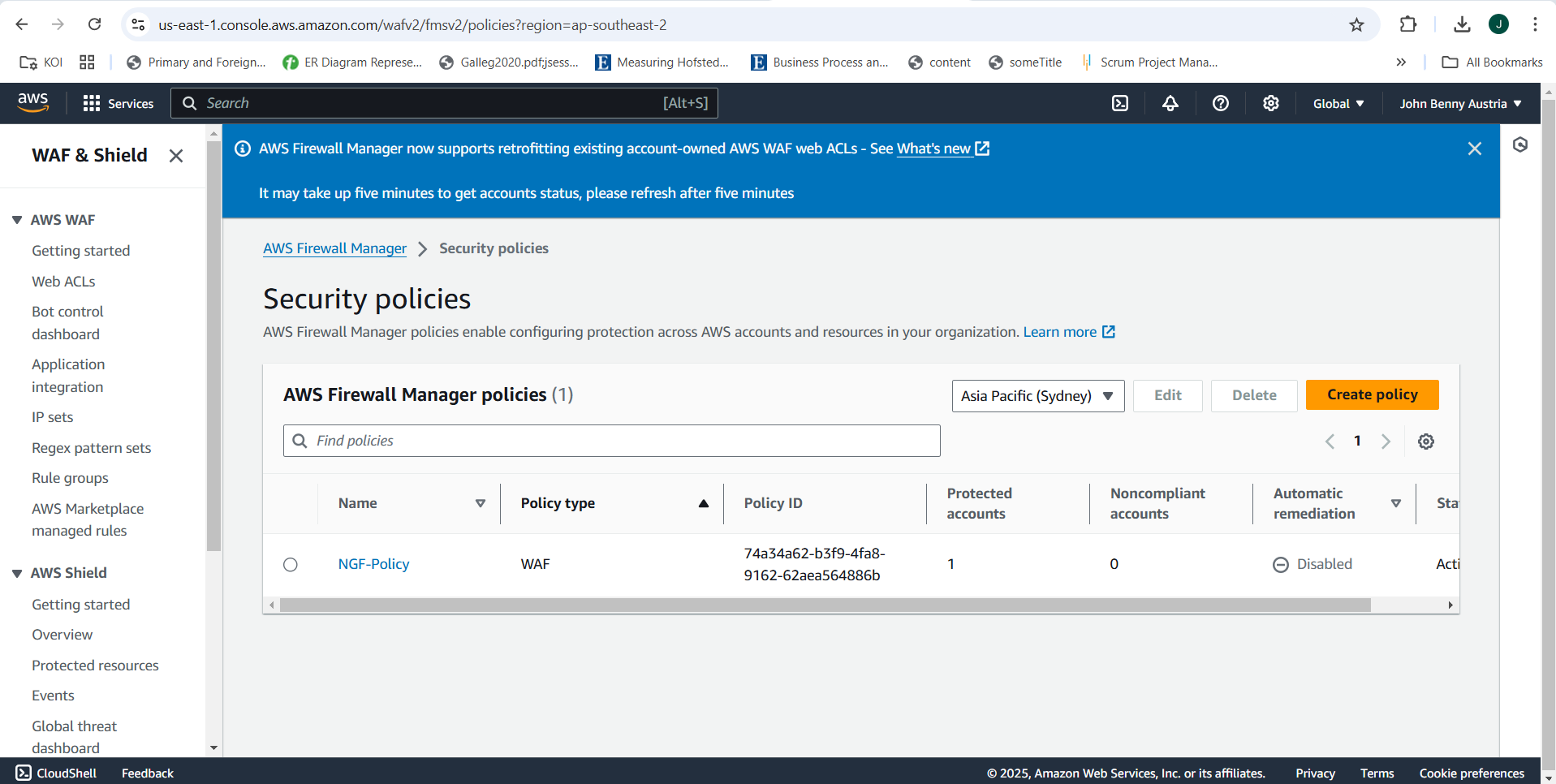


Figure ‑. NGF Firewall Security Policy

AWS Firewall Manager helps NGF WAF rules and Security Group settings consistent through all account and regions that are aligned in Northgate Financial Bank. The NGF Firewall Policy also protects the web application as it blocks SQL injections that are targeting the NGF’s application. EC2 instances are monitored through policy compliance and takes note of IP addresses that do not adhere to the bank’s security policies.

## Summary



Table ‑. AWS Services Summary

# CONCLUSION

This report offers comprehensive guidance and assistance for Northgate Financial's smooth transition to AWS cloud services. By leveraging AWS's scalability, security, and cost-efficiency, Northgate Financial can enhance its operations, boost productivity, and stay ahead in the competitive financial industry.

## Future Work

1. The migration to AWS is not the final step; ongoing system enhancement is crucial. Northgate Financial should consider the following actions post-AWS migration:

Leverage AWS Insights for Enhanced Decision-Making: Northgate Financial can utilize AWS-generated analytics and reports to make more informed decisions. These insights will assist the bank in refining its strategies, enhancing efficiency, and making data-driven choices to reach its objectives (Amazon Web Services, Inc., 2024).

1. Establish Access Control for Data Protection: While AWS's database services provide robust encryption, Northgate Financial should implement well-defined access control policies. By designating specific roles and permissions, the bank can ensure that sensitive financial data is accessible only to authorized personnel, minimizing the risk of security breaches (Amazon Web Services, Inc., 2024).
2. Enhance Data Management and Storage: Although AWS offers an image storage solution, Northgate Financial should strengthen its overall data management strategy. Given the vast amount of financial and customer information the bank handles, it's essential to improve backup and storage systems to maintain long-term data integrity (Amazon Web Services, Inc., 2024).
3. Develop a Tailored Disaster Recovery Plan: Despite AWS's disaster recovery service, Northgate Financial should create its own recovery plan customized to the bank's specific requirements. This plan should be regularly updated to address emerging risks and ensure swift recovery from any disruptions (Amazon Web Services, Inc., 2024).
4. Broaden Compliance Efforts Beyond HIPAA: AWS provides numerous compliance frameworks in addition to HIPAA that could benefit Northgate Financial. The bank should explore these standards and implement them to reinforce its security measures and safeguard sensitive financial data (Amazon Web Services, Inc., 2024).

## Plans for Extension

To ensure the smooth and efficient migration of Northgate Financial to AWS, it is necessary to implement the following measures to maintain security, efficiency, and compliance

1. Effective communication with stakeholders, such as banking officers and advisors, is necessary for Northgate Financial to communicate the upcoming shift to AWS. This includes clients, employees, and key stakeholders. During the migration, it's crucial to ensure that their sensitive financial data remains secure and compliant with industry standards like HIPAA.
2. Prior to the migration, Northgate Financial must update and review its data security protocols thoroughly. This must involve considering the identification of sensitive financial assets, carrying out a risk analysis and maintaining strict data access controls. High-level security measures should be implemented to differentiate between publicly available data and confidential information.
3. Regular Education of Workers: Given the technical nature of AWS and the need to adhere closely to financial laws, Northgate Financial should establish a training program for employees and clients. Individuals working in compliance, risk management or customer service should have the knowledge and tools to leverage AWS infrastructure. Training should be provided to clients in order for them to understand the impact of migration on their relationship with banks.
4. Thorough backup and data protection: With banking information being incredibly sensitive and heavily regulated, Northgate Financial must ensure a multi-layered backup plan is in place. Why? It is not recommended to store crucial data in a single storage location; instead, the company should ensure that its data is distributed across secure locations with diverse geographical coverage. This method will help to maintain the security of data integrity, prevent loss, and ensure business continuity in case of unexpected events.".
5. AWS provides comprehensive monitoring instruments for the bank's cloud-based platform, including Continuous Monitoring and Compliance Oversight. Northgate Financial must establish a robust monitoring system to detect security breaches or compliance risks in real-time. The bank will be able to respond promptly to any vulnerabilities by being monitored continuously, ensuring a secure, compliant, and efficient operation.

# REFERENCES

Amazon Web Services, 2024. Amazon EC2 Concepts. Amazon EC2 User Guide. Available at: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html [Accessed 15 January 2025].

Amazon Web Services, 2024. Amazon Virtual Private Cloud (VPC) User Guide. Available at: https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html [Accessed 15 January 2025].

Amazon Web Services, 2024. AWS CloudTrail User Guide. Available at: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html [Accessed 15 January 2025].

Amazon Web Services, 2024. AWS Firewall Manager. Available at: https://aws.amazon.com/firewall-manager/#:~:text=AWS%20Firewall%20Manager%20is%20a,and%20applications%20in%20AWS%20Organizations [Accessed 15 January 2025].

Amazon Web Services, 2024. AWS Key Management Service (KMS) Developer Guide. Available at: https://docs.aws.amazon.com/kms/latest/developerguide/overview.html [Accessed 15 January 2025].

Amazon Web Services, 2024. Introduction to AWS Identity and Access Management (IAM). Available at: https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html [Accessed 15 January 2025].

Amazon Web Services, 2024. Security Groups and Network ACLs - Best Practices. Available at: https://docs.aws.amazon.com/whitepapers/latest/aws-best-practices-ddos-resiliency/security-groups-and-network-acls-bp5.html [Accessed 15 January 2025].

Amazon Web Services, Inc., 2024. National Australia Bank Case Study. Available at: https://aws.amazon.com/solutions/case-studies/national-australia-bank-case-study/ [Accessed 15 January 2025].

AWS (2024). *Control traffic to resources using security groups - Amazon Virtual Private Cloud*. [online] docs.aws.amazon.com. Available at: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-security-groups.html.

Choudhary, A., Verma, P.K. and Rai, P., 2021. A walkthrough of amazon elastic compute cloud (Amazon EC2): a review. *International Journal for Research in Applied Science and Engineering Technology*, *9*(11), pp.93-97.

Juvonen, E., 2023. AWS Cost Management and Trend Analysis.

Mane, A.S. and Ainapure, B.S., 2021. Private Cloud Configuration Using Amazon Web Services. In *Information and Communication Technology for Competitive Strategies (ICTCS 2020) Intelligent Strategies for ICT* (pp. 839-847). Singapore: Springer Nature Singapore.

Moore, T.L., Conlon, S.S., Hewarathna, A.U. and Mailewa, A.B., Encryption Methods and Key Management Services for Secure Cloud Computing: A Review.

TechTarget, 2024. AWS Bucket. Available at: https://www.techtarget.com/searchaws/definition/AWS-bucket#:~:text=Share%20this%20item%20with%20your,object's%20name%2C%20URL%20and%20size [Accessed 15 January 2025].