Project Step 1

Joemar Lugtu – 301355179

Mark Labiano - 301346652

Jude Torres – 301350841

Syed - 301318212

School of Engineering Technology and Applied Science,

Centennial College

CBER 707: Cloud Security (section#: 002)

Professor Saeed Zamany

Introduction:

In this project, we delve into a hypothetical scenario involving Maple Bank, a prominent financial institution in the Greater Toronto Area, contemplating an expansion of its network infrastructure. Facing limitations with its current on-premises data center, Maple Bank has decided to leverage cloud computing technology, specifically Microsoft Azure, to facilitate the expansion. This initiative involves hosting most of their IT assets on the public cloud, opting for a hybrid cloud model by integrating their existing on-premises data center with Azure services. While this strategic move presents growth opportunities, it also introduces security apprehensions for the bank.

Benefits of hybrid cloud architecture:

- Facilitates Cloud Migration: Acts as an intermediate step for organizations transitioning from on-premises to the public cloud.
- Cost Savings: Optimizes resources, potentially leading to cost savings compared to exclusive on-premises or public cloud solutions.
- Regulatory Compliance: Ensures compliance with regulations by allowing organizations to retain sensitive data on-premises.
- Utilizes Existing Assets: Maximizes the value of existing on-premises assets while incorporating new public cloud resources.

- Workload Portability: Enables the movement of workloads across environments using containers and virtualization, providing deployment flexibility.
- Enhances Disaster Recovery and Resilience: Improves resilience, business continuity, and disaster recovery capabilities by deploying them across different environments.

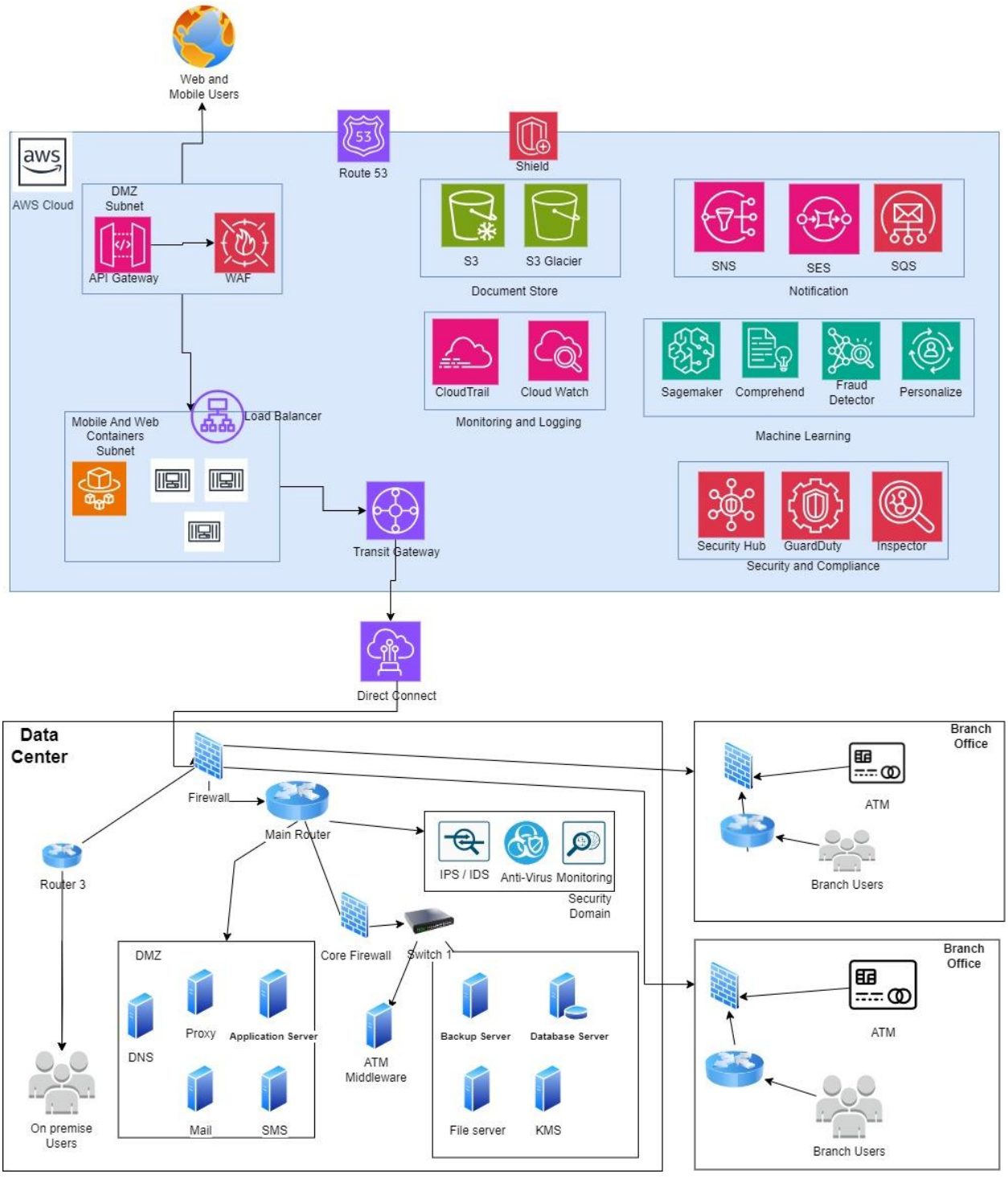

Fig: High Level Topology

Security Standards

ISO/IEC 27001: This standard provides a framework for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). It covers various aspects of information security, including data encryption, access control, network security, and compliance.

PCI DSS (Payment Card Industry Data Security Standard): The bank deals with credit card transactions, so compliance with PCI DSS is essential. This standard outlines specific security requirements for protecting cardholder data, including encryption, access control, and regular security testing.

NIST (National Institute of Standards and Technology) Cybersecurity Framework: Developed by NIST, this framework guides managing and reducing cybersecurity risk. It consists of five core functions: Identify, Protect, Detect, Respond, and Recover, which can help organizations establish a comprehensive security program.

SOC 2 (System and Organization Controls) Compliance: SOC 2 compliance ensures that service providers securely manage data to protect the interests of their customers. It focuses on security, availability, processing integrity, confidentiality, and privacy of customer data.

PIPEDA (Personal Information Protection and Electronic Documents Act): The bank operates in Canada or handles the personal information of Canadian citizens, compliance with PIPEDA is essential. Adhering to PIPEDA ensures that the bank appropriately manages and safeguards personal information, including data stored in AWS, under Canadian privacy laws.

CIS (Center for Internet Security) Controls: CIS Controls provide a prioritized set of actions for defending against the most common cyber threats. They cover various security domains, including inventory and control of hardware assets, continuous vulnerability management, and controlled use of administrative privileges.

AWS Well-Architected Framework: While not a traditional security standard, AWS Well-Architected Framework provides best practices for designing and operating secure, high-performing, resilient, and efficient infrastructure in AWS. It covers security considerations across various architectural pillars, including security, reliability, performance efficiency, cost optimization, and operational excellence.

Risk, Vulnerabilities, and Security Gaps to Mitigate

The bank should systematically identify and address potential security threats and vulnerabilities, ensuring the protection of its data in both AWS and on-premise environments while adhering to industry-recognized security standards. The following potential risks, vulnerabilities, and gaps were identified in the proposed solution and outline how each will be mitigated, referencing the security standards mentioned earlier:

1. **Risk: Unauthorized access to sensitive bank data.**
    - Vulnerability: Weak access controls or compromised credentials in both on-premise and AWS environments.
    - Mitigation: Implement robust access control mechanisms using IAM for AWS and centralized access control solutions for the on-premise data center, enforcing multi-factor authentication (MFA) for all users (referencing ISO/IEC 27001 and SOC 2).

2. **Risk: Data breaches due to lack of encryption.**
    - Vulnerability: Data at rest or in transit remains unencrypted in both environments.
    - Mitigation: Utilize encryption mechanisms such as AWS KMS for AWS and encryption protocols for on-premise data storage, ensuring data is encrypted at rest and in transit (referencing ISO/IEC 27001 and PCI DSS).

3. **Risk: Exposure to DDoS attacks leading to service disruptions.**
    - Vulnerability: Inadequate network security measures in both environments.
    - Mitigation: Implement DDoS protection measures such as AWS WAF and Shield for AWS and deploy dedicated DDoS mitigation solutions for the on-premise network infrastructure (referencing CIS Controls and NIST Cybersecurity Framework).

4. **Risk: Data residency and compliance violations.**
    - Vulnerability: Data stored in non-compliant locations in both AWS and on-premise environments.
    - Mitigation: Select compliant locations for data storage in both environments, ensuring adherence to regulations such as PIPEDA (for Canada) and GDPR (for EU) for both on-premise and AWS deployments, and implement data governance policies (referencing PIPEDA and GDPR).

5. **Risk: Insufficient disaster recovery preparedness.**
    - Vulnerability: Lack of multi-region redundancy and backup strategies for both environments.
    - Mitigation: Implement multi-region redundancy using AWS services like S3 Cross-Region Replication for AWS and deploy redundant backup solutions for on-premise systems, conducting regular disaster recovery drills for both environments (referencing ISO/IEC 27001 and CIS Controls).

6. **Risk: Insider threats compromising data integrity.**
    - Vulnerability: Privileged users abusing their access rights in both environments.
    - Mitigation: Enforce least privilege access controls and conduct regular access reviews for both AWS and on-premise systems, monitoring user activities using respective logging and monitoring solutions (referencing ISO/IEC 27001 and SOC 2).

7. **Risk: Failure to comply with industry standards and best practices.**
    - Vulnerability: Inadequate adherence to security frameworks in both environments.
    - Mitigation: Regularly assess compliance with standards such as ISO/IEC 27001, SOC 2, and CIS Controls for both on-premise and AWS deployments, and implement necessary controls to address gaps (referencing ISO/IEC 27001 and SOC 2).

8. **Risk: Lack of visibility into security events and incidents.**
    - Vulnerability: Ineffective monitoring and logging in both environments.
    - Mitigation: Implement comprehensive logging and monitoring solutions such as AWS CloudTrail and SIEM systems for both AWS and on-premise environments, establishing incident response procedures covering both areas (referencing ISO/IEC 27001 and NIST Cybersecurity Framework).

9. **Risk: Data loss or corruption due to improper backup procedures.**
    - Vulnerability: Inadequate backup and recovery mechanisms for both environments.
    - Mitigation: Implement automated backup solutions for AWS and on-premise systems, regularly testing backup integrity and recovery procedures in both environments (referencing ISO/IEC 27001 and SOC 2).
10. **Risk: Insecure configurations leading to vulnerabilities.**
    - Vulnerability: Misconfigured systems and services in both environments.
    - Mitigation: Implement configuration management and vulnerability assessment solutions for both AWS and on-premise systems, regularly auditing and remediating configuration drifts and vulnerabilities (referencing CIS Controls and NIST Cybersecurity Framework).

11. **Risk: Lack of employee awareness and training.**
    - Vulnerability: Employees unaware of security best practices in both environments.
    - Mitigation: Conduct regular security awareness training sessions for employees covering both AWS and on-premise security practices, providing clear security policies and procedures documentation for both environments (referencing ISO/IEC 27001 and SOC 2).

12. **Risk: Third-party service provider vulnerabilities.**
    - Vulnerability: Security weaknesses in AWS services or third-party integrations, as well as vendors supporting the on-premise environment.
    - Mitigation: Regularly assess the security posture of AWS services and third-party vendors through vendor risk assessments for AWS and on-premise systems, and implement contractual agreements to enforce security requirements for both environments (referencing ISO/IEC 27001 and SOC 2).

Security Controls

Incorporating security controls for both the on-premise data center and the AWS cloud environment ensures a comprehensive security posture. Here are detailed security controls to include in the solution:

1. **Access Control:**
    - Implement centralized identity and access management (IAM) solutions for both on-premise systems and AWS resources.
    - Enforce multi-factor authentication (MFA) for all user access.
    - Utilize role-based access control (RBAC) to ensure least privilege access.
2. **Data Encryption:**
    - Encrypt data at rest using appropriate encryption algorithms and key management practices for both on-premise storage systems and AWS.

- Implement secure data transmission protocols such as SSL/TLS for both on-premise and AWS data transfers.
- Utilize client-side encryption for sensitive data before transmission to AWS.

3. **Network Security:**
   - Implement firewalls, intrusion detection/prevention systems (IDS/IPS), and network segmentation to protect both on-premise and AWS environments.
   - Regularly monitor network traffic for anomalies and unauthorized access attempts.
   - Utilize network security appliances and services to protect against DDoS attacks in both environments.
4. **Data Residency and Compliance:**
   - Establish data residency policies and controls to ensure compliance with regulations such as PIPEDA or HIPAA for both on-premise and cloud environments.
   - Regularly audit and monitor data handling practices to ensure compliance with regulatory standards.
   - Implement data lifecycle management policies to govern data retention and disposal in both environments.

5. **Disaster Recovery and High Availability:**
   - Implement redundant systems and failover mechanisms in both on-premise and cloud environments to ensure high availability.

- Regularly test disaster recovery plans for both environments to ensure rapid recovery in case of data breaches or service disruptions.
- Utilize automated backup solutions for both on-premise and cloud-based data storage.

6. **Incident Response and Monitoring:**
    - Implement comprehensive logging and monitoring solutions for both on-premise and cloud environments using tools like SIEM (Security Information and Event Management).
    - Establish incident response procedures for both environments, including defined roles and escalation paths.
    - Conduct regular security assessments and penetration testing for both on-premise and cloud environments.
7. **Configuration Management:**
    - Implement configuration management tools and practices to ensure consistency and compliance with security standards for both on-premise and cloud-based systems.
    - Regularly review and update configurations based on security best practices and guidelines in both environments.
    - Utilize automated configuration management solutions for both on-premise and cloud environments.

8. **Backup and Recovery:**
    - Implement automated backup solutions for both on-premise and cloud-based data storage.
    - Regularly test backup integrity and recovery procedures to ensure data availability in both environments.
    - Store backup copies in geographically dispersed locations for added resilience in both environments.

9. **Security Awareness and Training:**
    - Conduct regular security awareness training sessions for employees covering both on-premise and cloud security best practices.
    - Provide clear security policies and procedures documentation for both environments and ensure employee compliance.
    - Encourage reporting of security incidents and suspicious activities in both environments.

10. **Third-Party Risk Management:**
    - Regularly assess the security posture of third-party vendors providing services for both on-premise and cloud environments.
    - Implement contractual agreements to enforce security requirements and standards for third-party vendors in both environments.

Monitor third-party access and activities to detect and mitigate potential security risks in both environments.

Prototyping a Technical Solution (Includes Security Implementation and Response Planning)

Technical Solutions:

1. **Cloud Infrastructure Setup**
    - Utilize AWS Management Console or AWS CLI to provision necessary cloud resources.
    - Configure subnets, route tables, and security group to control inbound and outbound traffic.

2. **Identity and Access Management (IAM)**
    - Deploy IAM roles and policies to securely control access to AWS services.
    - Enforce the least privilege principle by only giving users, groups, and roles the permissions they require.
    - To improve security, allow Multi-Factor Authentication (MFA) for IAM users.

3. **Data Encryption**
    - Use third-party SSL certificates or AWS Certificate Manager to implement TLS encryption for data in transit.

4. **Network Security**
    - Employ AWS Firewall Manager or AWS WAF (Web Application Firewall) to defend against DDoS attacks and common web vulnerabilities.

- To manage traffic flow and limit access to important resources, set up AWS Security Groups and Network Access Control Lists (NACLs).
- To connect privately to AWS services without disclosing data to the public internet, use AWS PrivateLink.

Security Implementation:

1. **Security Monitoring and Incident Detection**

- Configure AWS CloudWatch to log and monitor AWS resources centrally.
- Set up CloudWatch alarms to send out alerts when there are unusual activity, sudden spikes in resource usage, or security breaches.
- Use machine learning techniques to continuously detect and analyze threats with AWS GuardDuty.

2. **Security Patching and Vulnerability Management**

- To find and fix security flaws in the cloud environment, use AWS Inspector or other third-party vulnerability scanning tools.

Response Planning:

1. Incident Response Team

- Form an incident response group of cloud architects, IT security experts, and important bank stakeholders.

- Assign duties and obligations to investigators, incident coordinators, and communication liaisons within the team.

2. Incident Response Plan

- Create a thorough incident response strategy that outlines the steps you take in order to identify, evaluate, and address security incidents in the AWS cloud.
- Provide pre-established communication channels, escalation pathways, and incident classification standards based on impact and severity.

3. Incident Detection and Analysis

- Put in place automatic alerting systems to instantly alert the incident response team to possible security incidents.
- Use distributed tracing and log analysis with AWS CloudWatch Logs Insights and AWS X-Ray to find the source of security events.

4. Incident Containment and Mitigation

- Isolate impacted resources or services as soon as a security incident is detected to stop additional unauthorized access or data compromise.
- For automated incident response tasks like reducing compromised resources or changing security groups, use AWS CloudFormation or AWS Lambda.

5. Communication and Notification

- Create channels of contact with AWS support, governing bodies, and impacted clients to coordinate incident response activities both within and externally.

- Send out regular updates and alerts to all relevant parties about the incident's status, the repair process, and the preventive measures that are being put in place.

6. **Post-Incident Analysis and Remediation**
    - To find lessons learned, areas for improvement in security controls and procedures, and a root cause analysis, conduct a comprehensive post-incident investigation.

To reduce recurrence of such situations, put corrective measures in place. These could include changing security configurations, reviewing policies, or improving personnel training.