Conduct an Application Security Review

Executive Summary

The purpose of this security audit is to make sure that the company architecture is compliant with SOX and PCI/DSS frameworks. Since we're dealing with customers' information, we have to make sure that all data is designed and protected following the CIA triad: confidentiality, Integrity and Availability. What's more, the audit also reveals some weaknesses in the systems that need to be addressed such as default configuration, unencrypted data in transit and data at rest, lack of access control, backups and loggings, etc.

Risk 1: *Default configuration for PostgreSQL*

Risk Rating: *Medium*

Related Security Frameworks (if any)

Explanation of Risk
It is important to change the configuration of the PostgreSQL database as it poses a risk of exposing sensitive data. Documentations of default configuration are widely available in public. Therefore, if an attacker can get to the database, they will have access to sensitive data. Despite its high impact, this is considered medium because the database is in the internal infrastructure, which costs attackers a lot of resources to compromise the system.

Recommendations **(Include at least two. Or, if only giving one, explain why that is the only feasible solution.)**	**How does the recommendation mitigate the risk?**
Change Default configuration	Configure the database to follow the best practices of the company. This will take attackers more resources to access the database
Implement Access Control with least privileges.	Only appropriate roles can get access to the database. This will ensure that only personnels with related tasks can access the database
Use complex passwords, which include upper case, lower case, numbers, special characters and avoid using common password phrases (password, admin, root)	In the event of a user with access to the database being compromised, having complex passwords adds another layer to prevent attackers from accessing the database.

Risk 2: *Unencrypted data in transit*

Risk Rating: *Critical*

Related Security Frameworks (if any): *PCI SSD*

Explanation of Risk
Because there are no SSL certificates, there are chances the traffic across the network is intercepted. If attackers successfully penetrate the internal network, they can intercept the traffic and use them as leverages to perform other attacks. Also, all sensitive information will be revealed. This violates the PCI SSD framework, whose objectives are to protect the confidentiality and integrity of customers' data.

Recommendations **(Include at least two. Or, if only giving one, explain why that is the only feasible solution.)**	**How does the recommendation mitigate the risk?**
Use the latest version of TLS (1.3) to encrypt data in transit. Whether	TLS 1.3 is the latest version that is being used to encrypt data in transit. With this implementation, attackers cannot intercept traffic across the network, hence protecting the sensitive data. By doing this, the company can guarantee the integrity and confidentiality of data.
Use VPN	Because traffic is forwarded from a public cloud AWS, a VPN connection will ensure the traffic is encrypted. Also, VPN can be used in parallel with authentication protocols to ensure that only employees connecting to the internal network have access to the database (data analysts and Customer Relationship Managers)

Risk 3: *Unencrypted data at rest*

Risk Rating: *Critical*

Related Security Frameworks (if any): PCI DSS

Explanation of Risk
Without encrypting the database, the company violates PCI DSS framework as it fails to preserve the confidentiality of users' information. Once attackers get access to the database, they will be able to obtain sensitive information.

Recommendations **(Include at least two. Or, if only giving one, explain why that is the only feasible solution.)**	**How does the recommendation mitigate the risk?**
Encrypt data within the database with strong encryption keys like AES256	By encrypting the data, the company can make sure that even if attackers get access to the database, they can't view sensitive information. This not only preserves the confidentiality of data, but also complies with PCI DSS.
Enable Database-level encryption	Many database management systems offer built-in encryption features. Enable these features to encrypt data at the database level, which can provide a higher level of security and minimize the risk of accidental exposure. This adds extra layers of protections to the data.
Implement Intrusion Detection System (IDS)	We should implement an IDS specifically designed to monitor and protect databases. These can help detect and prevent unauthorized access attempts or suspicious activities. Special firewall rules should be created to allow connections from AWS, Internal Customer Management Page and the internal workstations.

Risk 4: *Lack of Loggings*

Risk Rating: *Critical*

Related Security Frameworks (if any): SOX

Explanation of Risk
SOX framework requires financial companies to track data breach attempts, keep event logs readily available for auditors. Because at the moment, there is no logging implemented, the company is violating SOX compliance.

Recommendations **(Include at least two. Or, if only giving one, explain why that is the only feasible solution.)**	**How does the recommendation mitigate the risk?**
Implement Intrusion Prevention System / Intrusion Detection System (IPS/IDS) to monitor traffic from public cloud AWS	It is important to monitor the connections from outside the network as they contain more risks.By implementing a logging system, we are able to keep track of important events like users' loggins, data

	exchange, access controls, etc., which consequently improves the company's security postures.
Another Logging system should also be implemented for Customer Relationship Managers and data analysts.	From within the corporate's network, we should also monitor all traffic. This not only helps to detect and respond to malicious activities, but also complies with the SOX for logging and auditing purposes.
Centralized logging	Because we monitor connections from different surfaces, we need a centralized logging system to collect and ingest data for management and analysis.
Log Storage	For auditing purposes, we need to define a log storage strategy that includes retention policies. Have the log rotated regularly and archived according to SOX's requirements.
Access Control	Logs should be only authorized to personnels who manage them. This prevents attackers from modifying logs in case they get a hold of the logging systems. Having access control also complies with the SOX framework.
Regular review and auditing	According to the SOX framework, a company should demonstrate compliance within 90-day cycles. Regularly reviewing and analyzing logs not only complies with the SOX framework but also helps the company identify security incidents in a timely manner.

Risk 5: *Lack of data backups*

Risk Rating: *Critical*

Related Security Frameworks (if any): PCI DSS

Explanation of Risk
In every organization, having one database is not enough. Without a backup, in case of a security incident, the company won't be able to protect the data integrity. This also violates the PCI DSS policies. Because this is not compliant with the framework, it needs to be addressed immediately.

Recommendations **(Include at least two. Or, if only giving one, explain why that is the only feasible solution.)**	**How does the recommendation mitigate the risk?**
Create a backup for the database	Maintain regular backups of your encrypted database and store them securely. In the event of a security incident, having recent backups can help you restore your data without compromising its integrity.
Create a segmented network inside the company for the database.	Put the database in a segmented network to increase security. In case the internal network is compromised, the segmented network adds another layover of protection to the database.

Risk 5: *Lack of protections against common web attacks*

Risk Rating: *High*

Related Security Frameworks (if any)

Explanation of Risk
Since users can modify their information by sending data through a web portal, it is important to protect the whole network from common web attacks like SQL injection, Cross-Site Scripting, File Inclusions, etc.

Recommendations **(Include at least two. Or, if only giving one, explain why that is the only feasible solution.)**	**How does the recommendation mitigate the risk?**
Place a Web Application Firewall (WAF) in front of the Web Portal which users use to update their information.	The WAF will prevent common attacks like SQl Injection, XSS, File Inclusion, DDos, etc. Having the WAF in place reduces the attack surfaces and helps the company maintain the application's availability, integrity and confidentiality.

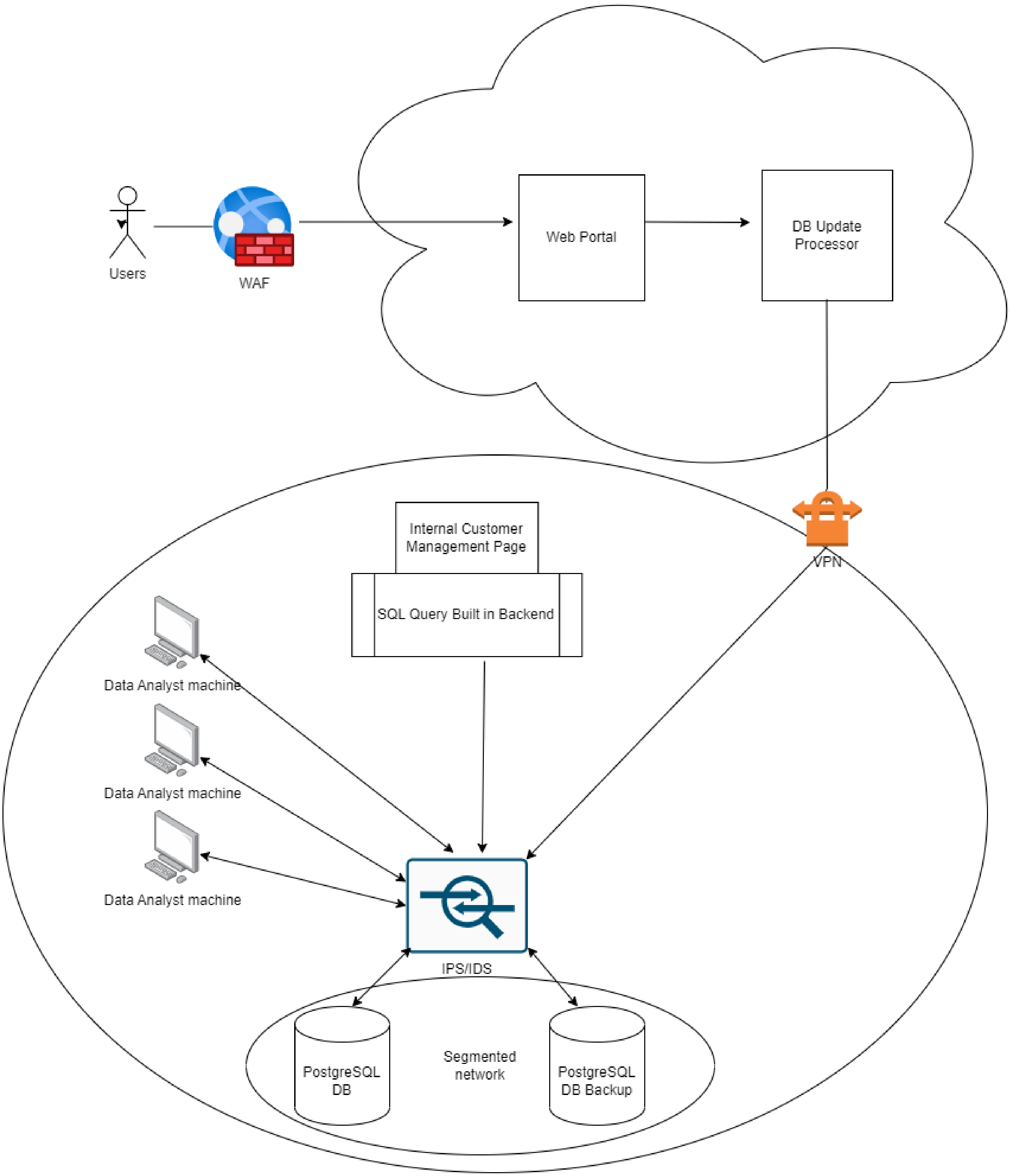
Final Architecture Recommendation

In summary, the general issues are that some of the security practices do not meet requirements from both SOX and PCI/DSS frameworks: unencrypted data in transit and at rest, lack of backups, no logging implementations and lack of access control.

- To encrypt data in transit, we use TLS for all the traffic across the network. On top of that, we add extra security by having all traffic encrypted in VPN tunnels.
- To encrypt data at rest, we enforce strong encryption like AES-128 or AES-256. Also, we enable database-level feature, which pre-exist in the database management system.
- We also have another backup of the PostgreSQL so in case of an incident, the company's operations won't be disrupted.
- We also implement IDS/IPS to monitor traffic and detect malicious activities. In case of intrusion, the system will block malicious attempts.

It doesn't cost much to implement these security controls. In return, these changes will make sure that the system is compliant with both SOX and PCI/DSS. Not only do they help the company avoid fines but also improve the company's overall security postures.

Beside those recommendations, we can also implement MFA for users who use the web portal as well for employees within the company. MFA implementations will enhance the authentication protocols.



Users
WAF
Web Portal
DB Update Processor
VPN
Internal Customer Management Page
SQL Query Built in Backend
Data Analyst machine
Data Analyst machine
Data Analyst machine
IPS/IDS
PostgreSQL DB
Segmented network
PostgreSQL DB Backup