جامعة أم القرى
UMM AL-QURA UNIVERSITY

Eagle’s eye

Cyber security company

MANAR ALSAMILY
FATMAH AL-HUSIEEN
WAFAA ALAWADHI
RETAJ BAAQEEL
RAZAN FARIS

ABOUT OUR COMPANY

organization's name is **Eagle's eye.**

And it's a cyber security company with three categories of its services. The first category is:

cyber security operation and it has the following:

- GRC
- penetration testing
- SOC

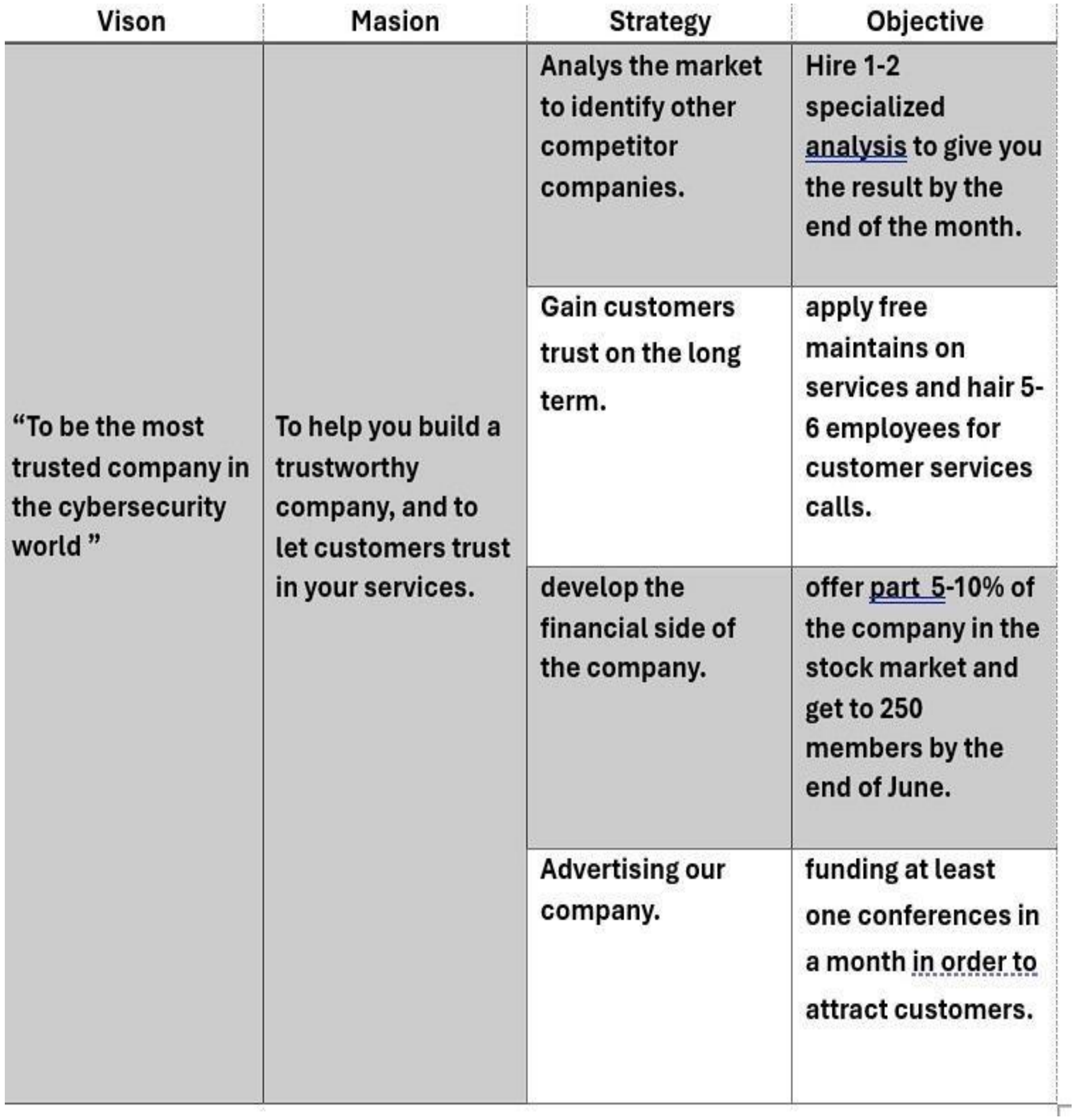
THE SECOND CATEGORY IS cloud computing protection, and it has the following:

- Web application firewall (WAF)
- Protection from denial-of-service attacks (DDOS)

The third category is data protection, and it has the following:

- prevent data theft (DLP)
- E-mail protection.

Data strategy:



Vison	Masion	Strategy	Objective
“To be the most trusted company in the cybersecurity world ”	To help you build a trustworthy company, and to let customers trust in your services.	Analys the market to identify other competitor companies.	Hire 1-2 specialized analysis to give you the result by the end of the month.
		Gain customers trust on the long term.	apply free maintains on services and hair 5-6 employees for customer services calls.
		develop the financial side of the company.	offer part 5-10% of the company in the stock market and get to 250 members by the end of June.
		Advertising our company.	funding at least one conferences in a month in order to attract customers.

Data governance policy

Purpose: the purpose of the policy is to establish a clear, robust, and dynamic framework for the effective management and protection of Eagle's Eye Company data assets, by outlining guidelines, procedures, and responsibilities. Through adherence to this Policy, Eagle's Eye Company enhances data-driven decision-making and maintains trust with stakeholders

Scope: This Policy applies to everyone involved with Eagl's Eye company, including employees, contractors, consultants, and third-party partners who access or use Eagl's Eye data. It covers all data owned, handled, or sent by Eagl's Eye company, no matter its form or where it's located, and the equipment and software used for these tasks.

It also includes data stored or used in applications, even if they're in hosted environments where Eagle's Eye company doesn't control the technology infrastructure directly:

Roles and responsibilities

company personnel must access and use data only as required for the performance of their job functions, not for personal gain or for other inappropriate purposes; they must also access and use data according to the security levels assigned to the data. (Failure to comply makes you vulnerable to penalties and accountability)

Data Owne:

The Data Owner, as designated by Eagl's Eye company, establishes, and maintains data policies, standards, and rules in alignment with business needs and regulatory requirements. They hold ultimate responsibility for overseeing the management and usage of data within .the organization

Data Controller:

The Data Controller, appointed by Eagl's Eye company, sets forth technical requirements and guidelines for the implementation of data policies and standards. They ensure that data is processed and managed in .accordance with specified technical protocols

Data Custodian:

The Data Custodian, designated by Eagl's Eye company, manages data storage systems and access controls to safeguard the confidentiality, integrity, and availability of data. They are responsible for the secure storage, retrieval, and disposal of data assets.

Data Processor:

The Data Processor, authorized by Eagl's Eye company, analyzes data to generate insights, reports, or visualizations that support decision-making processes. They transform raw data into actionable information to facilitate informed business decisions.

Data Steward:

The Data Steward, appointed Eagl's Eye company, oversees the implementation of data governance policies and ensures adherence to quality requirements. They are responsible for maintaining data integrity, accuracy, and compliance with organizational standards.

Process 1: Data Classification

Data Classification Policy**:**

Purpose: The purpose of this data classification policy is to establish a framework for categorizing and protecting data based on its impact and sensitivity within Eagle's Eye, a cyber security company. The policy aims to ensure that data is appropriately handled, stored, and accessed in accordance with the organization's security requirements.

Scope: This policy applies to all employees, contractors, and third-party entities who handle or have access to data within Eagle's Eye. It covers all data repositories, including physical and digital formats.

data classification levels:

1 .Top Secret:

-Data classified as "Top Secret" has the highest level of sensitivity and requires the utmost protection. Unauthorized access or disclosure of this data could have severe and irreparable consequences for Eagle's Eye and its clients. Examples include classified research, trade secrets, sensitive customer information, and other highly confidential data.

2 .Secret:

-Data classified as "Secret" is of significant importance and requires strict access controls. Unauthorized access or disclosure of this data could have a serious impact on the organization's operations and potentially compromise client confidentiality. Examples include internal documents ,proprietary methodologies, non-public business plans, and other moderately sensitive information.

3 .Restricted:

-Data classified as "Restricted" has a lower level of sensitivity but still requires safeguards to prevent unauthorized access or disclosure. While the impact of unauthorized disclosure may be limited, it could still have negative consequences for Eagle's Eye or its clients. Examples include publicly available but sensitive information, internal communications ,project updates, and other data that should be handled with care.

4 .Public:

-Data classified as "Public" has no significant sensitivity and can be freely disclosed without adverse effects on the organization or its clients .This category includes information intended for public consumption, such as marketing materials, general website content, public announcements ,and other non-confidential data.

Data Classification Process:

Step 1: Identify all data of Eagle's Eye

-Prepare an inventory of all the data owned by Eagle's Eye, including data related to Cyber Security Operations, Cloud Computing Protection, and Data Protection.

Step 2: Appoint Responsible for Performing Data Classification

-Assign the responsibility for data classification to a specific person, such as the Data Protection Officer or a designated cybersecurity expert at Eagle's Eye, who understands the data and its value in the context of cybersecurity services.

Step 3: Conduct Impact Assessment Process

3.a: Identify the Impact Category

-Identify the main and subcategories of potential impacts specific to

cybersecurity services:

-Cyber Security Operations:

-GRC (Governance, Risk, and Compliance)

-Penetration Testing

-SOC (Security Operations Center)

-Cloud Computing Protection:

-Web Application Firewall (WAF)

-Protection from Denial of Service Attacks (DDOS)

-Data Protection:

-Data Loss Prevention (DLP)

-Email Protection

3.b: Identify the Impact Level

-Assign a level of impact to each potential impact based on parameters such as impact duration, difficulty to control the damage, time to recover and repair, and size of the impact.

-Levels of impact:

-High Impact: Extremely grave or serious long-term damages that cannot be recovered or rectified.

-Medium Impact: Grave or serious long-term damages that are difficult to control.

-Low Impact: Limited or intermittent short-term damages that can be controlled.

-No Impact: Unlikely to cause any long- or short-term damage.

Step 4: Identify Relevant Laws and Regulations (only if impact level is Low)

-Study whether the disclosure of data conflicts with applicable laws and regulations, such as data protection laws, industry compliance standards ,and any specific regulations related to cybersecurity services.

-If disclosure conflicts with laws and regulations, classify the data as "Restricted".

Step 5: Balance between Benefits of Disclosure and Negative Impacts (only if the answer to Step 4 is "NO")

-Assess the potential benefits of disclosure and determine if they outweigh the negative impacts.

-If benefits are greater than negative impacts, classify the data as "Public".

-If benefits are less than negative impacts, classify the data as "Restricted".

Step 6: Review Classification Level

-Have a data classification reviewer from Eagle's Eye's data management office or cybersecurity team review the assigned classification level within one month of the initial classification.

Step 7: Apply Appropriate Controls

-Apply relevant controls based on the classification level to ensure data protection for each service category.

Process 2: Incident Response Process Process Explanation:

A process refers to a sequence of steps or actions undertaken to achieve a specific objective. In the context of incident response, it involves the systematic approach to handling and responding to security incidents,ensuring the organization can effectively detect, contain, and minimize the impact of any security breaches or data incidents.Incident Response Policy:

Purpose:

The purpose of this incident response policy is to establish a structured approach for detecting, responding to, and recovering from security incidents within Eagle's Eye, a cyber security company. The policy aims toensure the organization can effectively manage and mitigate the impact of incidents on data privacy and security.

Policy for Incident Response Process:

1 .Incident Identification and Reporting:

-Clear guidelines should be established for employees to identify and report potential security incidents promptly. This includes specific channels and contacts for reporting incidents, such as a designated incident response team or IT department.

2 .Incident Categorization and Prioritization:

-Incidents should be categorized based on their severity, impact on data privacy, and potential consequences for Eagle's Eye and its clients. A prioritization framework should be established to focus resources on addressing high-priority incidents promptly.

3 .Incident Response Team and Roles:

-Designated incident response team members should be identified with clearly defined roles, responsibilities, and escalation procedures. This includes decision-making authority, incident containment, evidence collection, and coordination with relevant stakeholders.

4 .Incident Investigation and Analysis:

-Procedures should be in place to conduct thorough investigations of security incidents. This includes preserving evidence, analyzing the incident's root cause, and determining the extent of the breach or privacy violation.

5 .Incident Containment and Recovery:

-Response activities should focus on containing the incident, minimizing further damage, and restoring normal operations. This may involve isolating affected systems, patching vulnerabilities, restoring backups, or implementing additional security measures.

6 .Incident Reporting and Communication:

-Appropriate communication channels and procedures should be established to notify affected individuals, regulatory authorities, and other

stakeholders as required. The policy should also address internal communication and reporting to executive management and the board of directors.

Extra Component: Lessons Learned and Continuous ImprovementEagle's Eye recognizes the importance of continuous improvement in its data classification and incident response processes. To foster a culture of learning and enhancement, the following component is included:

1 .Lessons Learned and Post-Incident Analysis:

-After each significant incident, a post-incident analysis should be conducted to identify lessons learned, root causes, and areas for improvement. This analysis should involve the incident response team , relevant stakeholders, and subject matter experts. Findings and recommendations from the analysis should be documented and incorporated into future incident response plans and training programs.

By incorporating this component, Eagle's Eye aims to foster a proactive approach to data protection and incident response, continually refining its processes to enhance the organization's overall security posture.

Data Lifespan Management Standards:

1 .Penetration testing reports are retained for 5 years after the last interaction.

2 .Vulnerability scan reports are retained for 3 years after the last interaction.

3 .Customer personal data is retained for 7 years after the last interaction, then archived for an additional 3 years before being destroyed.

Data Quality Standards :

1 .Customer data must be verified directly with the customer every six months.

2 .The customer must fill out all required personal information fields on the first request. Unless it’s been over 10 years since last interaction.

3 .Customer phone numbers must be submitted in the format "+966XXXXXXXXX" with the leading 0 removed.

4 .All data entries must be less than 60 days old to be considered timely.

Security and Privacy Standards:

1 .All credit card information is encrypted using AES-256 encryption.

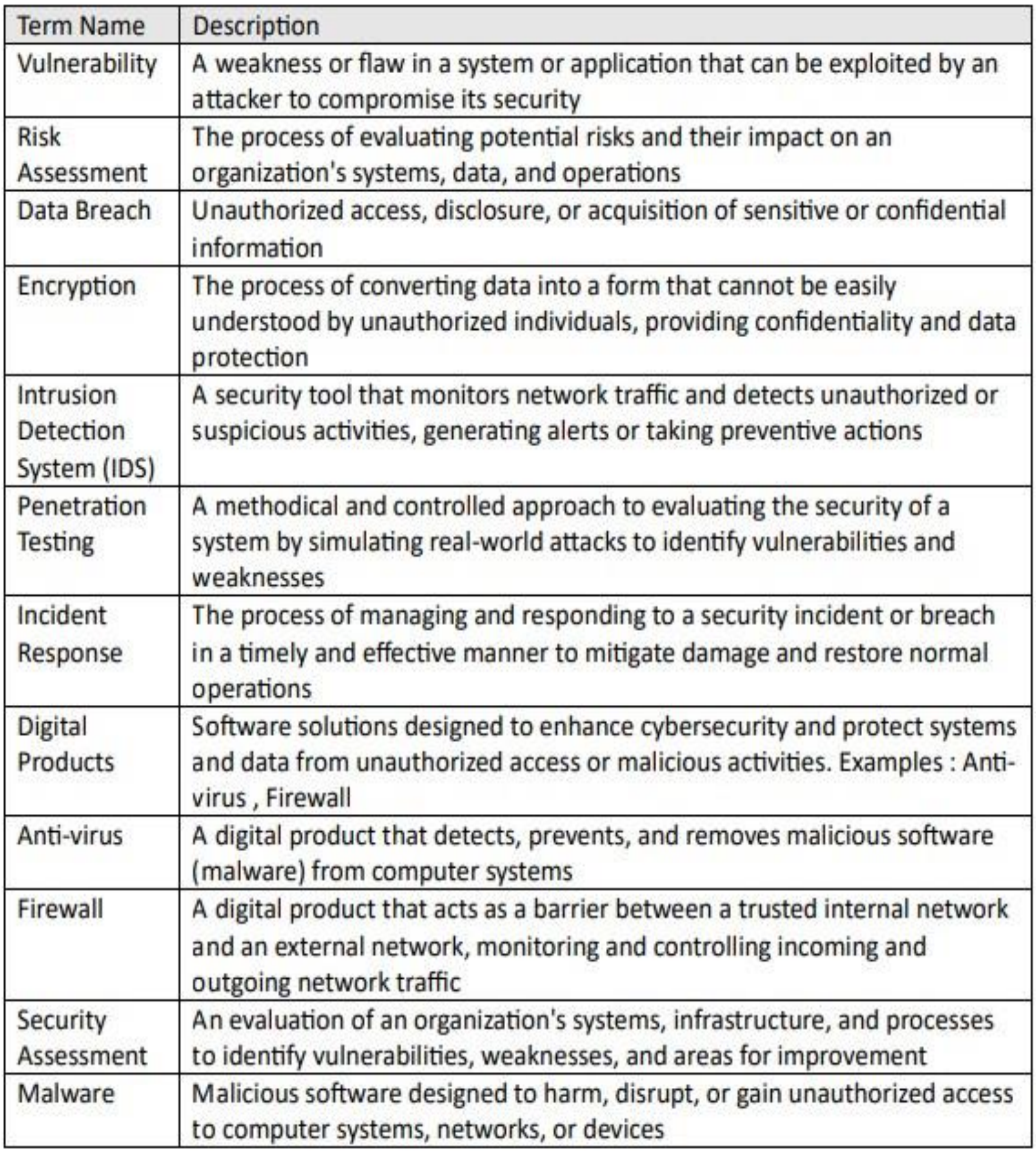
2 .Multifactor authentication is required to access any systems containing customer personal data.

3 .Annual audits are conducted to ensure compliance with GDPR and other relevant data protection regulations.

Another fields of Standards:

1 .All employees must wear at least one article of clothing that incorporates the company logo. Ties, and hats, and abaya are acceptable options.

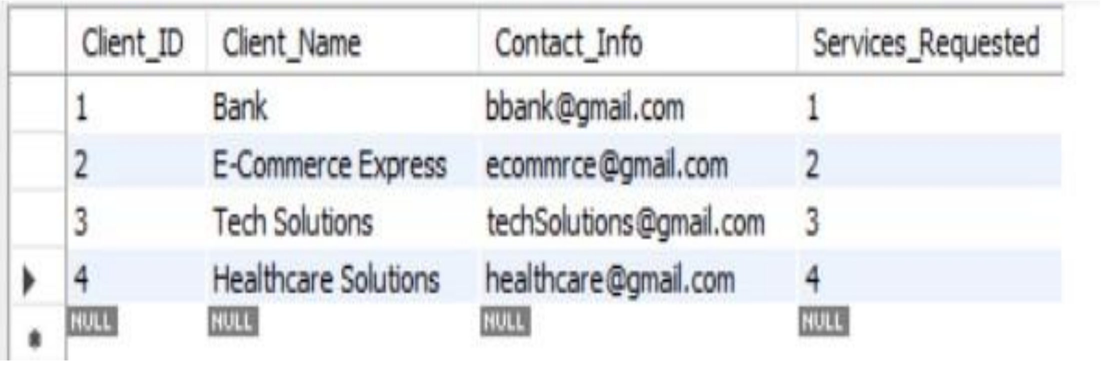
Data Glossary:



Term Name	Description
Vulnerability	A weakness or flaw in a system or application that can be exploited by an attacker to compromise its security
Risk Assessment	The process of evaluating potential risks and their impact on an organization's systems, data, and operations
Data Breach	Unauthorized access, disclosure, or acquisition of sensitive or confidential information
Encryption	The process of converting data into a form that cannot be easily understood by unauthorized individuals, providing confidentiality and data protection
Intrusion Detection System (IDS)	A security tool that monitors network traffic and detects unauthorized or suspicious activities, generating alerts or taking preventive actions
Penetration Testing	A methodical and controlled approach to evaluating the security of a system by simulating real-world attacks to identify vulnerabilities and weaknesses
Incident Response	The process of managing and responding to a security incident or breach in a timely and effective manner to mitigate damage and restore normal operations
Digital Products	Software solutions designed to enhance cybersecurity and protect systems and data from unauthorized access or malicious activities. Examples : Anti-virus , Firewall
Anti-virus	A digital product that detects, prevents, and removes malicious software (malware) from computer systems
Firewall	A digital product that acts as a barrier between a trusted internal network and an external network, monitoring and controlling incoming and outgoing network traffic
Security Assessment	An evaluation of an organization's systems, infrastructure, and processes to identify vulnerabilities, weaknesses, and areas for improvement
Malware	Malicious software designed to harm, disrupt, or gain unauthorized access to computer systems, networks, or devices

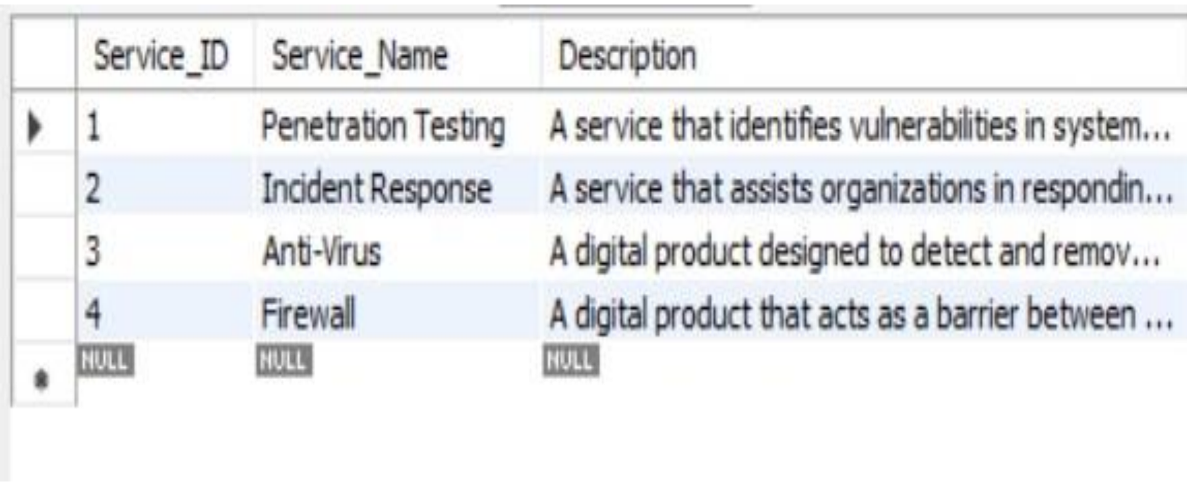
Data Dictionary:

Clients Table



	Client_ID	Client_Name	Contact_Info	Services_Requested
	1	Bank	bbank@gmail.com	1
	2	E-Commerce Express	ecommrce@gmail.com	2
	3	Tech Solutions	techSolutions@gmail.com	3
▶	4	Healthcare Solutions	healthcare@gmail.com	4
*	NULL	NULL	NULL	NULL

Security Services Table



	Service_ID	Service_Name	Description
▶	1	Penetration Testing	A service that identifies vulnerabilities in system...
	2	Incident Response	A service that assists organizations in respondin...
	3	Anti-Virus	A digital product designed to detect and remov...
	4	Firewall	A digital product that acts as a barrier between ...
*	NULL	NULL	NULL

Data Inventory:

In Eagle's Eye Company, data inventory is considered a vital tool for ensuring data security and integrity and understanding how to better use it. Data inventory helps identify the types of available data, their sources, usage patterns, access permissions, and more. This facilitates strategic decision-making, the development of security strategies, data analysis, and the improvement of internal processes.
data inventory at Eagle's Eye Company serves as the foundation for effective data management and ensures safe and appropriate data usage, thereby contributing to enhancing organizational performance and successfully achieving strategic objectives.

Roles:

- Security Services Manager: This role is entrusted with overseeing data management and security operations within the organization. They ensure that access to client information is appropriately restricted and that data quality standards are always maintained.

- Security Operations Coordinator: As the coordinator responsible for managing the catalog of security services offered by the company, this role ensures that service information remains current and accurately reflects the range of services available to clients.

Data Governance:

- A robust set of data governance policies is established and diligently enforced to safeguard the security, privacy, and integrity of the organization's data assets.

- Strict data access controls are implemented, ensuring that only authorized personnel have access to sensitive information, thereby minimizing the risk of unauthorized access or data breaches.

- Regular data quality assessments and audits are conducted to identify and rectify any discrepancies or inconsistencies in the data, ensuring that it remains accurate and reliable.

- Clearly defined data retention policies specify the duration for which data should be retained, as well as the procedures for securely disposing of data when it is no longer needed.

- Metadata management practices are meticulously maintained to document and organize information about the data, facilitating its effective use and management across the organization.

Relationships:

In the Clients Table, the Service_Requested column serves as a foreign key referencing the

Service_ID column in the Security Services table. This relationship establishes a connection between client data and the corresponding security services requested, facilitating efficient data management and retrieval.

Additional Information:

- Both the Clients and Security Services tables are integral parts of the " *Eagle's Eye Company* " database, essential for the organization's day-to-day operations.

- Access to these tables is strictly restricted to authorized personnel within the Security Operations Team, with access permissions meticulously managed by the IT department to uphold data security standards.

- Regular backups of the database are conducted weekly on Sundays by the proficient Database Administration team, ensuring data availability and resilience against potential data loss incidents.

- Data retention policies mandate that client information must be retained for a minimum period of 5 years, in compliance with regulatory requirements and industry standards.

- The database undergoes annual security audits conducted by external auditing firms to assess and ensure compliance with prevailing standards and regulations, reinforcing the organization's commitment to data security and regulatory compliance.

- Comprehensive data asset protection measures are implemented to safeguard data assets from unauthorized access, loss, or corruption, thereby preserving their integrity and value to the organization.

- Data asset valuation techniques are employed to assess the significance and strategic importance of data assets to the organization's operations and objectives.

- Metadata documentation, meticulously maintained by the Data Governance team, provides valuable insights and context about the organization's data assets, aiding in their effective management and utilization.

Name	Description	Source	Format	Owner	PK	Data Usage
Clients Table	Contains information about clients of Eagle's Eye Company	Internal data collected during client registration process.	Database table	Security Services Manager	Client_ID	Client information is used to maintain communication and provide services tailored to client needs.
Security Services Table	contains information about security services offered by Eagle's Eye Company	Internal data maintained by the Security Operations Team.	Database table	. Security Operations Coordinator	Service_ID	Service information is used to determine the availability of security services and assist clients in selecting appropriate services.

Table 1(showing detailed information about the use of data in each table, showing the main fields, owners, source, and description of each table in Eagle's Eye Company database.)

Column Name	Data Type	Location	Description
Client_ID	INT, PK	In EagleEyeDB Clients Table	Unique identifier for each client
Client_Name	VARCHAR	In EagleEyeDB Clients Table	Name of the client
Contact_Info	VARCHAR	In EagleEyeDB Clients Table	Contact information of the client
Services_Requested	INT, FK	In EagleEyeDB Clients Table	Services requested by the client, referencing the Service_ID in the Security Services table.
Service_ID	INT, PK	In EagleEyeDB SecurityServices Table	Unique identifier for each service
Service_Name	VARCHAR	In EagleEyeDB SecurityServices Table	Name of security service offered
Description	TEXT	In EagleEyeDB SecurityServices Table	Description of the security service

Table 2(showing column locations clearly within Eagle's Eye Company's database.)

Regulatory and Compliance:

How our organization “Eagle’s eye” manages to comply with the PDPL:

- Step1- we make sure all the team members understand article 1 terms which they define the regulation, personal data, processing, collecting, etc. and what does each term involve.

- Step2- in “Eagle’s eye” we classify our data the right way. By knowing what data, we have, and categorizing our data based on its sensitivity level, it will make the compliant process a lot more easer. Also, when processing the data we follow the Key Obligations mentioned in the PDPL:

a. Data Minimization: we only collect the and process the necessary amount of data.
b. Transparency: we inform the data subject about the purpose of the collection and how we will use their data.
c. Consent: we make sure that we have the individual consent before processing their information.
d. Data Subject Rights: we respect the data subject right to access, correct, delete, their data at any time.

e. Data Breaches: in “Eagle’s eyes “ we promise to inform the data subject about any data breaches that effect their personal, financial, ..information.

• Step3- Data Security: in a lot of cases our company counts as a third-party company, so we make sure that we implement the strongest security measure.

a. Data Encryption: we implement encryption on our data when transferring and at rest (on the servers).
b. Strong Access Controls: we make sure to implement strong role-based access controls, and we use multi-factor authentication, and other tools.
c. Network Security: before providing other companies with network security tools, we make sure our company has some like firewalls, intrusion detection systems, and other security tools.
d. Regular Security Assessments: we use penetration testing, regular vulnerability scans, and security audits to identify and address vulnerabilities.

• Step4- Data Retention Policies: we make sure we have a clear policy statement about retain personal data and how it will be disposed of. As mentioned in the PDPL

. • Step5- Incident Response Plan: we developed a robust and comprehensive incident response plan that can handle any security incident effectivel

FMEA:

Process	*Failure mode*	*Cause*	*Effect*	*Measures and control*	*S (1-10)*	*O (1-10)*	*D (1-10)*	*PRN*
Incident response	Lack of Documentation	Lack of standardized documentation procedures	difficult to locate information and increasing the risk of overlooking crucial details.	Implement standardized documentation procedures and	7	5	4	210
	Failed Incident Containment	Lack of clear containment strategies or procedures	Escalation of Impact	Develop clear containment strategies and procedures	8	6	4	336
	Incorrect Incident Classification	Lack of employee experience	Wrong instruction followed to deal with it	Provide training, support, and monitoring	9	7	3	252
	Incorrect Incident Classification	lack of clear criteria or guidelines	may be misjudged, response don't match the actual severity or nature of the incident.	Establish clear criteria and guidelines for classification	8	7	6	336
	Inadequate Incident Analysis	Lack of employee experience	Ineffective Remediation	Provide training and resources for incident analysis	9	7	6	280
	No update for incident response plan	Lack of awareness of the need for plan updates	the company can’t response new threats or attack	Regularly review and update incident response plan	10	9	6	432

identify risk:

Financial Risk:

- Unexpected Costs: Increased expenses due to unforeseen incidents or over-budget projects.
- Revenue Loss: Potential loss of clients or contracts leading to reduced income.
- Investment Risk: Poor investment decisions impacting the company's financial stability.
- Insurance Risk: Insufficient coverage for operational or cyber incidents.

Service Delivery or Operational Risk:

- Service Downtime: Unplanned outages impacting service availability.
- Data Loss: Loss of critical data due to system failures or breaches.
- Incident Response Failures: Inadequate response to security incidents or breaches.
- Quality Control Failures: Inconsistent service quality impacting customer satisfaction.

People / HR Risk:

- Talent Shortage: Difficulty in attracting and retaining skilled cybersecurity professionals.
- HR Compliance: Non-compliance with labor laws and regulations.
- Employee Misconduct: Fraud, negligence, or other misconduct by employees.
- Performance Management: Ineffective performance appraisal systems.

Information Risk:

- Data Breaches: Unauthorized access to sensitive information.
- Information Leakage: Accidental or deliberate leaks of confidential information.
- Data Privacy Violations: Breaches of data protection laws and regulations.
- Insider Threats: Risks posed by employees or contractors with access to sensitive information.

Strategic / Policy Risk:

- Regulatory Changes: New regulations impacting business operations.
- Reputation Damage: Strategic missteps harming the company’s reputation.
- Policy Changes: Ineffective internal policies affecting business efficiency.
- Stakeholder Misalignment: Misalignment between stakeholders’ expectations and company strategy.

Stakeholder Satisfaction / Public Perception Risk:

- Customer Dissatisfaction: Poor service delivery leading to customer dissatisfaction.
- Client Relationships: Strained relationships with key clients.
- Service Quality: Perception of service quality affecting customer loyalty.
- Expectation Gaps: Mismatches between stakeholder expectations and service delivery.

Legal / Compliance Risk:

- Regulatory Compliance: Non-compliance with cybersecurity laws and regulations.
- Contractual Obligations: Breaches of contract terms with clients or partners.
- Intellectual Property: Violations of intellectual property rights.
- Data Protection Laws: Non-compliance with data protection regulations.
- Licensing Issues: Problems with software or technology licenses.

Technology Risks:

- System Failures: Failures of critical IT systems and infrastructure.
- Software Bugs: Defects in software affecting performance and security.
- Integration Issues: Problems integrating new technologies with existing systems.
- Cyber Attacks: Threats from hackers and malicious software.
- Data Center Risks: Risks associated with data center operations.
- Disaster Recovery Failures: Inadequate disaster recovery and business continuity plans.

Information risk

- Data Breaches: Unauthorized access to personal data.
- Data Misuse: Improper use of personal data.
- Data Minimization: Collecting and retaining excessive amounts of personal data.
- Anonymization Issues: Problems with anonymizing data effectively.
- Cross-border Data Transfer: Risks associated with transferring personal data across borders.

Security Risk:

- Phishing Scams: Attempts to acquire sensitive information through deceit.
- Ransomware: Attacks that encrypt data and demand ransom for its release.
- DDoS Attacks: Distributed Denial of Service attacks disrupting operations.
- Weak Authentication: Inadequate authentication mechanisms.
- Network Vulnerabilities: Weaknesses in network security.

جامعة أم القرى
UMM AL-QURA UNIVERSITY