ORGANIZATIONAL CYBERSECURITY REPORT

FINAL REPORT

Tanishq Milind Borse

CSEC 603 – ENTERPRISE SECURITY

PROF. BILL STACKPOLE

ROCHESTER INSTITUTE OF TECHNOLOGY

2024

Table of Contents

List of Tables

List of Figures

1. Executive Summary

This Organizational Cybersecurity Report for AWS is a comprehensive assessment that delineates the current security posture, identifies potential vulnerabilities, and proposes strategic solutions to mitigate risks. The report is guided by rigorous standards such as NIST and ISO/IEC 27001, ensuring that our security measures are robust and adhere to global best practices. The main objective is to fortify our defenses against identified vulnerabilities that pose the highest risk to our operations, thereby protecting our assets, customer trust, and market position. Our analysis reveals critical vulnerabilities within the AWS infrastructure that could lead to significant operational disruptions and financial penalties. The vulnerabilities range from misconfigured S3 buckets to inadequately managed IAM roles, each carrying the potential for unauthorized data exposure. In response, we have categorized and prioritized these vulnerabilities based on their impact and developed a tailored response that includes a tiered budget approach to address them effectively. The financial strategy involves three primary budget scenarios—low-cost, medium-cost, and high-cost—each designed to balance risk mitigation with cost efficiency. These budget plans are constructed to ensure that the most critical vulnerabilities are addressed first, with flexibility to scale up defenses as needed. This structured financial approach not only ensures comprehensive coverage but also optimizes the allocation of resources towards the most impactful security measures. To enhance AWS's cybersecurity framework, we recommend strengthening forensic capabilities, expanding endpoint detection, enhancing encryption practices, and integrating advanced AI and machine learning tools. These initiatives will improve our ability to preemptively identify and respond to threats, ensuring that AWS can continue to provide secure, reliable, and scalable cloud services. Moving forward, it will be crucial to maintain a dynamic reassessment of our security measures to adapt to the evolving cyber threat landscape and protect our long-term value and reputation.

The recommendations provided in this report are geared towards not just compliance but ensuring that AWS can continue to lead in the cloud computing space with trust and integrity. By implementing these recommendations, AWS will enhance its defensive capabilities and align its cybersecurity measures with its overarching business objectives, thereby securing its infrastructure and customer data against current and future cyber threats.

2. Methodology

In architecting our cybersecurity budget, we've employed a multi-layered methodology, informed by established frameworks like NIST[iii] [iii]and ISO/IEC 27001[ivv]. This provides us with a comprehensive roadmap to prioritize investments in security measures that can dramatically reduce risk exposure. Our methodological cornerstones include:

Structured Approach: We break down our cybersecurity needs into detailed tasks, ensuring a clear prioritization from core network defenses to advanced threat detection and end-user compliance.

Cost Assessment: Our financial estimations blend AWS's detailed pricing with market benchmarks from sources like Glassdoor, offering an accurate and realistic budget projection.

Risk-Centric Allocation: By appraising risks using established standards, we allocate our budget towards controls that address the most significant threats, ensuring efficient use of resources.

Strategic Alignment: Every budget item is chosen to align with our long-term cybersecurity strategy, reflecting our commitment to a robust and adaptive security posture.

Evolutionary Budgeting: Recognizing the dynamic nature of cyber threats, we commit to continuous evaluation and adjustment of our budget, informed by the latest cybersecurity research and industry developments.

Data-Driven Insights: The budget is detailed in an accompanying spreadsheet, categorized into Low, Medium, and High-Cost plans, derived from comprehensive online research and salary data. While exact figures are estimated, they provide a solid foundation for understanding AWS’s cybersecurity financial requirements.

For further insights into these frameworks, readers are encouraged to explore the official NIST and ISO/IEC 27001[vi] websites.

There is a spreadsheet that has these budget calculations attached to this report. There are multiple sheets labelled as Low-Cost Budget, Medium-Cost Budget, and High-Cost Budget. These costs are based on information found on google searches, and Glassdoor salaries[vii]. The cost of tools and salaries are approximately educated guesses based upon relevant information found on the internet, a lot of these data are not publicly available and hence approximating these values can give us a good understanding of the security budgets of Amazon Web Services.

3. Introduction to AWS

a. Enterprise History

Amazon is an American multinational technology company that focuses on e-commerce, cloud computing and digital streaming to name a few. It has been one of the most influential economic and cultural forces in the world. It was founded by Jeff Bezos from his garage in Bellevue, Washington on 5th of July 1994. It started as a online marketplace for books but has now expanded into a several other product and service categories. The journey of this 28-year-old company has been a remarkable one and it has now become one of the world's most valuable brands. [viii]

Although the company is best known among consumers for its retail platform, most of its operating profits (as of 2024) come from its cloud computing division, Amazon Web Services (AWS). Amazon is also emerging as a leader in generative artificial intelligence (GenAI) with its Bedrock platform. Amazon is in the streaming wars with its Prime Video entertainment and sports subscription model—including original content—battling for share of viewers.[ix]

Amazon's beginnings are rooted in its third-party seller services, subscription services, and advertising. It has long said it aims to expand sales by "improving all aspects of the customer experience, including lowering prices, improving availability, offering faster delivery times, increasing selection, expanding product information, improving ease of use, and earning customer trust," according to Securities and Exchange Commission (SEC) filings.

The Fig 1.01 shows the history of amazon's company milestone, product launches, and acquisitions from its initial stages to 2022. On 27th Nov 2023 the company surpassed FedEx and UPS to become the number one delivery company in the US. [x]

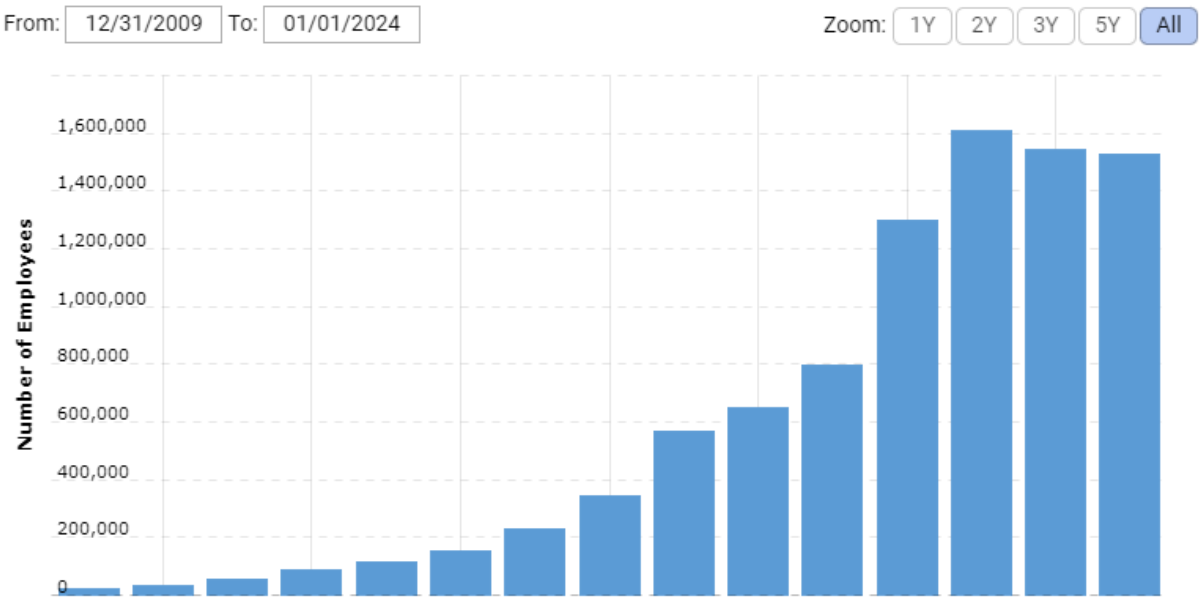

Fig. 1.01 – Number of employees

Sector	Industry	Market Cap	Revenue
Retail/Wholesale	Internet Commerce	$1751.209B	$574.785B

Fig. 1.02 – Market Capital

b. Market Positions

Amazon is predicted to become the largest US retailer in 2024, with a projected global Prime membership reaching around 300 million by the end of the year, an increase from over 200 million reported previously. The company's e-commerce market share at the end of 2023 is expected to be 42.2%, marking a significant increase year-over-year. Amazon's e-commerce dominance is underscored by its significant market share, which at one point was more than double the combined share of its nine closest competitors, including major retailers like eBay, Walmart, and Apple. JPMorgan estimates show that, in 2023, Amazon's gross merchandise volume, or GMV, will grow 11.6% year-over-over to $477 billion. JPMorgan estimates that there will be about 300 million Prime members globally by the end of this year. In 2021, then-CEO Jeff Bezos said the company had "more than 200 million Prime members worldwide." Amazon also has a massive grip on the e-commerce marketplace and, at the end of 2023, JPMorgan analysts

expect the company's e-commerce market share to be 42.2%, an increase of 106 basis points year-over-year

c. Business Models

Since its founding, Amazon has expanded its business by acquiring several companies, such as the audiobook company Audible in 2008, the livestreaming platform Twitch in 2014, the grocery chain Whole Foods Market in 2017, and the home security company Ring in 2018. Amazon operates various business units that span retail—which includes both online and physical stores—advertising, cloud computing through AWS, logistics, payments, and B2B services, showcasing its broad and diverse business model.

In 2023, Amazon reported nearly $575 billion in total revenues and a net profit exceeding $30 billion. Online retail was a major contributor, accounting for over 40% of Amazon's total revenues, while Third-party Seller Services and Physical Stores also made significant contributions. Additionally, segments like Amazon Web Services, Subscription Services, and Advertising have become rapidly growing parts of the business, significantly boosting Amazon's overall financial performance.

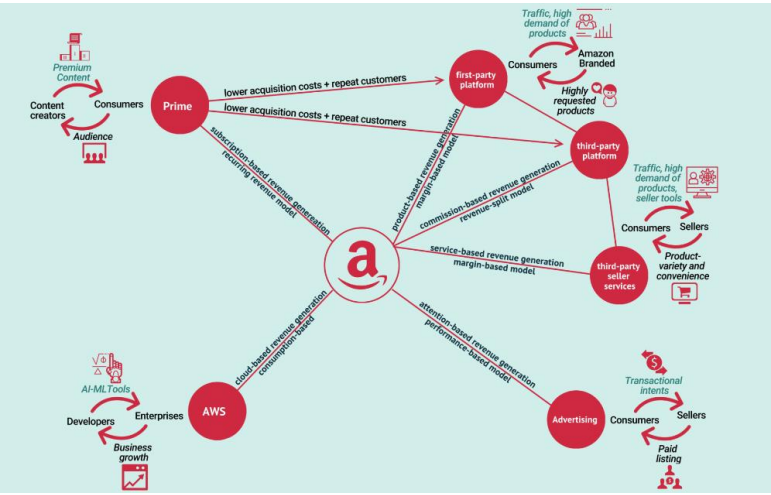

Fig. 1.04 – Revenue Model

Amazon operates across five distinct business models simultaneously. Firstly, it acts as an e-commerce platform, where it not only sells its own products but also offers a marketplace for third-party sellers. Secondly, Amazon operates a major enterprise cloud platform through AWS (Amazon Web Services). Thirdly, it manages a subscription service, Amazon Prime, which provides various benefits to subscribers. Fourthly, Amazon provides advertising services on its platform, especially for third-party sellers looking to increase their visibility. Lastly, Amazon is

also a hardware manufacturer, creating products like the Alexa voice assistant, the Kindle ebook reader, and more.[xi]

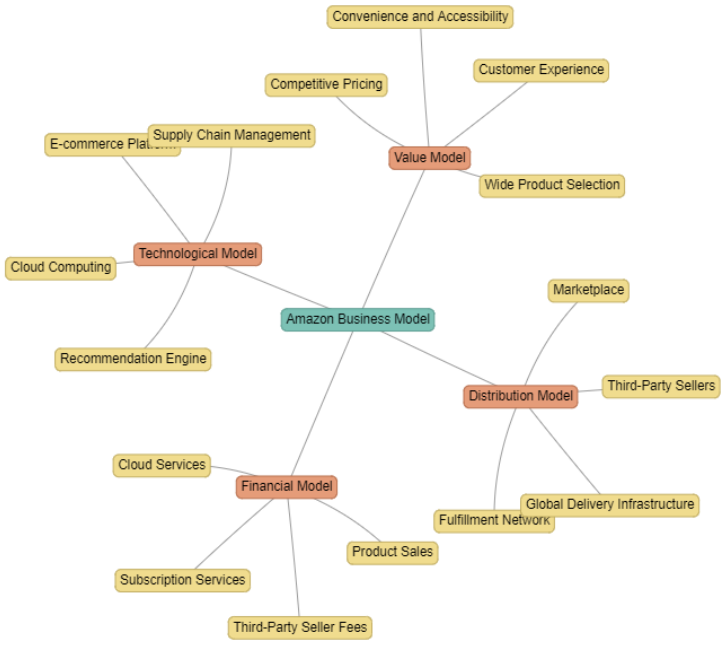

Fig. 1.04 – Business Model

d. Financial Information

In the first quarter, Amazon reported that its cloud division, Amazon Web Services (AWS), experienced a remarkable 17% increase in revenue year over year, reaching $25.04 billion. This growth exceeded Wall Street's expectations, with analysts surveyed by StreetAccount predicting revenues around $24.49 billion. This performance marks a significant acceleration from the 13% growth reported in the previous quarter for AWS.

As Amazon continues to dominate the e-commerce landscape, it has also solidified its position as a pivotal player in the information technology sector. AWS has become a critical infrastructure provider for a diverse range of clients including major corporations, startups, and government agencies, offering extensive computing resources, database software, and networking services. Notably, AWS contributed 17% to Amazon's total revenue of $143.313 billion.

Additionally, AWS has proven to be a lucrative endeavor for Amazon, largely due to the high margins typically associated with software services. In this quarter, AWS generated $9.42 billion in operating income, constituting about 62% of Amazon's total operating income. This figure surpasses the expectations of analysts polled by StreetAccount, who had forecasted an operating income of $7.52 billion for AWS.

Moreover, AWS's operating margin reached an impressive 37.6%, marking the highest level since at least 2014, underscoring its efficiency and profitability within the broader Amazon portfolio.[xiixiii]

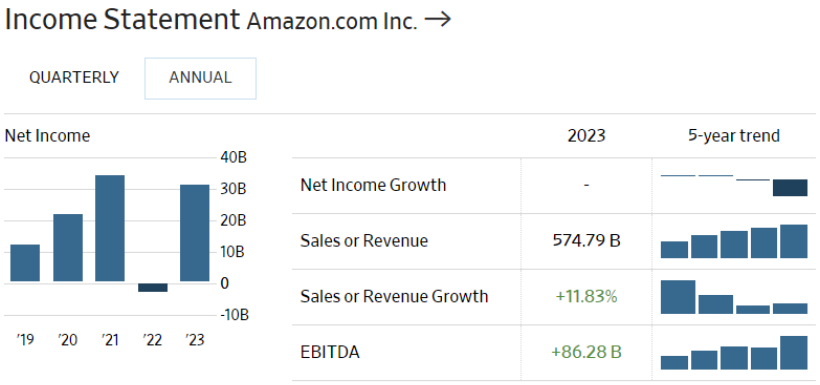

Fig. 1.05 Amazon Net Income vs EBITDA

The complete income statement is available on the website which showcases a revenue of 574,785 million USD with a gross profit of 270,046 million USD.[xiv]

Amazon Revenue Breakdown	2023
Online stores	$231.87B
Physical stores	$20.03B
Third-party seller services	$140.05B
Subscription services	$40.21B
AWS	$90.76B
Advertising	$46.9B
Other	$4.96B

Table. 1.00 – Revenue Breakdown

e. Company values vs AWS Security Model

Amazon AWS follows a platform business model that gains traction by tapping into network effects. Born as an infrastructure built on top of Amazon's infrastructure, AWS has become a company offering cloud services to thousands of clients from the enterprise level to startups. And its marketplace enables companies to connect to other service providers to build integrated solutions for their organizations.

Amazon generated over half a trillion dollars in revenue in 2023, of which $231.87B from online stores, over $140.05B from third-party seller services, $90.76B from AWS, $46.9B from advertising, $40.21B from subscription services, $20.03B billion in physical stores, and $4.96B from other sources.

That makes AWS a perfect target for Malicious threat actors, so for the purpose of this risk assessment, we will be primarily focusing on Vulnerabilities revolving around Amazon Web Services.

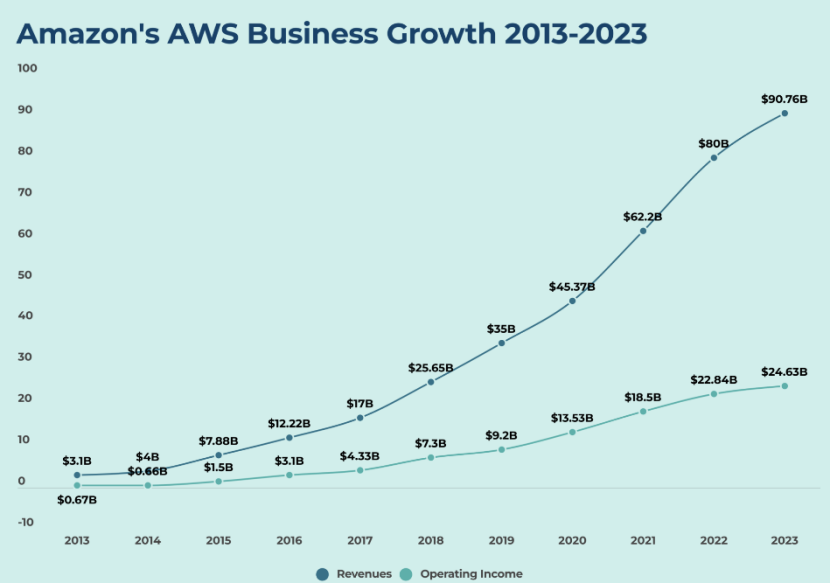

Fig. 1.06 – AWS Business growth

As Amazon AWS becomes the infrastructure for thousands of startups and SaaS companies, it shares its distribution capability by integrating other services providers to enable other companies to benefit from solutions that go well beyond the cloud.

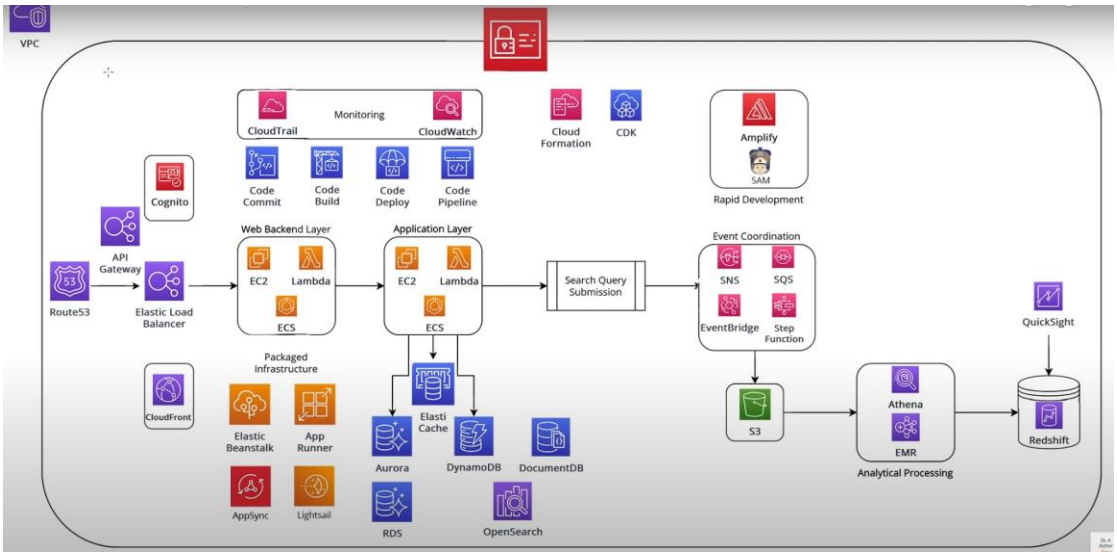

Fig. 1.07 – AWS Core Services

Shared Responsibility Model: In AWS's Shared Responsibility Model, both AWS and the customer play integral roles in ensuring security and compliance. AWS eases the operational load for the customer by handling the operation, management, and control of everything from the host operating system and virtualization layer down to the physical security of the facilities where the services operate. On the other hand, customers are responsible for managing the guest operating system, which includes regular updates and security patches, as well as any applications they run and the configurations of AWS's security group firewalls.

Customers need to make informed decisions about the services they use since their specific responsibilities will vary based on the chosen services, how those services are integrated into their existing IT environments, and the relevant legal and regulatory requirements. This model not only divides responsibilities clearly but also offers the flexibility and control customers need to effectively manage their part of the security operations. This approach delineates the responsibilities into two main categories: Security "of" the Cloud, which AWS manages, and

Security "in" the Cloud, which customers handle

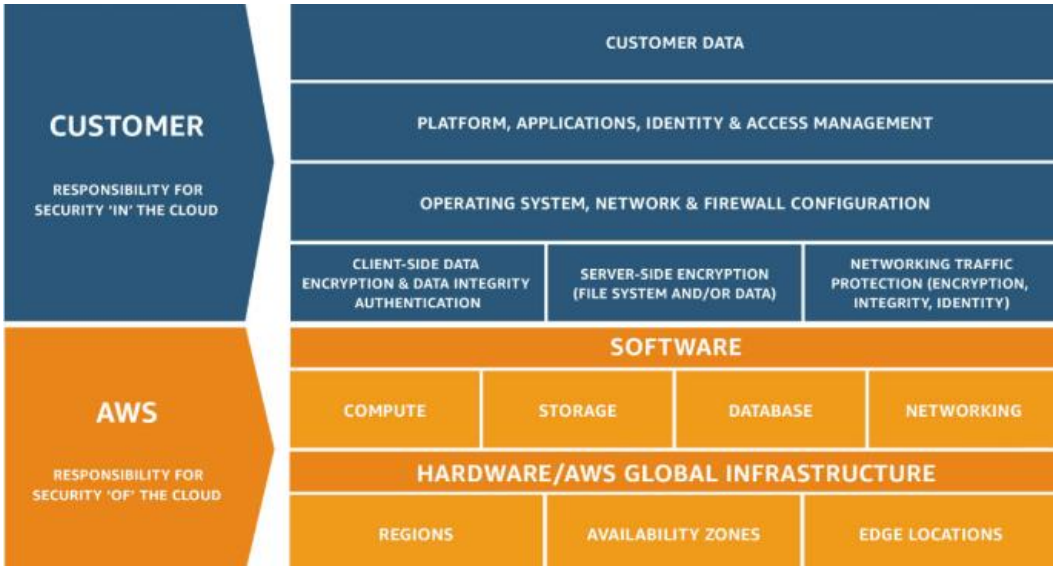

Fig. 1.08 – Shared Responsibility Model

In AWS's shared responsibility model, the division of security duties is clear-cut. AWS takes on the "Security of the Cloud" — this means AWS is in charge of securing the underlying infrastructure that powers all the services in the AWS Cloud. This includes everything from the physical hardware and software to the networking components and the facilities where these services operate.

On the other hand, the "Security in the Cloud" is the responsibility of the customer. This responsibility varies based on the services they choose to use. For instance, with Infrastructure as a Service (IaaS) offerings like Amazon EC2, customers are responsible for several aspects of security. This includes managing the operating system, including updates and security patches, any applications they install, and the settings of the AWS-configured firewalls known as security groups. For more abstract services like Amazon S3 or Amazon DynamoDB, while AWS manages the infrastructure and platforms, customers need to handle their data security, classify their assets, and manage permissions using IAM tools.

The model also extends to IT controls. Both AWS and its customers share the responsibility for managing and operating the IT environment. AWS can take on some of the customer's burdens by managing physical infrastructure controls, allowing customers to focus on what they deploy

in the cloud. This sharing of responsibilities means customers can leverage AWS's documentation to help manage their part of the security, ensuring a comprehensive approach to safeguarding their applications and data on AWS.[xv]

4. Identification of Assets

For assessing the risk of any enterprise, it is important that we identify and classify the assets that are valuable to them.

a. AWS Core Services:

Amazon Web Services (AWS) provides a comprehensive suite of global cloud-based products that cater to various aspects of computing needs, from computing power and storage to databases and analytics. These tools are designed to help organizations accelerate their operations, reduce IT expenses, and easily scale according to their needs. For anyone looking to quickly launch applications, AWS's core services such as computing, storage, and networking are essential and provide the foundation needed for nearly every application, whether new or existing.[xvi]

Here's a breakdown of the core services AWS offers:

Compute: AWS provides options to rent virtual machines or execute code based on specific events, with Amazon Elastic Compute Cloud (EC2) being the flagship service.

Storage: For data storage and retrieval in various formats, AWS offers Amazon Simple Storage Service (S3), which is known for its object-based storage capabilities.

Databases: AWS services include options for setting up, operating, and scaling both relational and NoSQL databases, prominently featured through Amazon Relational Database Service (RDS).

Analytics: For analyzing large datasets to extract insights, Amazon Redshift offers a powerful data warehousing solution.

Networking: Services like Amazon Virtual Private Cloud (VPC) enable users to link their resources and applications to the internet and manage web traffic.

Mobile: Amazon Pinpoint supports the development, testing, and deployment of mobile applications, also providing mobile analytics.

Developer Tools: AWS enhances development efficiency through tools like AWS CodePipeline, which supports continuous integration and continuous delivery.

Management Tools: AWS CloudWatch helps users monitor and manage their AWS resources effectively.

IoT: For Internet of Things applications, AWS IoT Core offers a managed platform that facilitates secure communications between connected devices.

Security: Amazon Identity and Access Management (IAM) helps users secure their AWS resources by managing access permissions.

Enterprise Applications: Amazon Workspaces allows the building, deployment, and management of enterprise-grade applications on a virtual desktop.[xvii]

These services not only help organizations streamline and optimize their operations but also support the ongoing evolution of their IT capabilities as they progress in their cloud adoption journey. Many customers start with these fundamental services to establish their applications on AWS, leveraging additional AWS offerings to further refine and expand their cloud infrastructure.[xviii]

b. Infrastructure assets:

AWS's global infrastructure is one of its most significant assets, consisting of the AWS Global Cloud Infrastructure, which provides over 200 fully featured services from data centers worldwide. This infrastructure includes AWS Regions and Availability Zones, ensuring high availability, fault tolerance, and scalability for applications. AWS's global network of data centers and related physical assets have around 105 Availability Zones within 33 geographic regions, with announced plans for 18 more Availability Zones and six more AWS Regions in Malaysia, Mexico, New Zealand, the Kingdom of Saudi Arabia, Thailand, and the AWS European Sovereign Cloud.[xix]

c. Data assets:

Customer data stored across AWS services, including personal and sensitive information. AWS Systems Manager's features, such as Application Manager and AppConfig, help manage and remediate issues with resources in the context of applications, offering insights into deployment status, resource configurations, and operational issues. This reflects AWS's approach to managing data assets across multicloud and hybrid environments. With Systems Manager Automation, you can author custom runbooks with a low-code visual designer or choose from over 370 predefined runbooks provided by AWS. You can run Python or PowerShell scripts as part of a runbook in combination with other automation actions such as approvals, AWS API calls, or running commands on your EC2 instances.

AWS Systems Manager Incident Manager enables faster resolution of critical application availability and performance issues. It helps you prepare for incidents with automated response plans that bring the right people and information together. With Incident Manager, you can automatically take action when a critical issue is detected by an Amazon CloudWatch alarm or

Amazon Event Bridge event. Incident Manager executes pre-configured response plans to engage responders via SMS and phone calls, links designated chat channels using AWS Chatbot, and executes AWS Systems Manager Automation runbooks. Incident Manager helps you improve service reliability by suggesting post-incident action items, such as automating a runbook step or adding a new alarm, based on Amazon's post-incident analysis template.

d. System assets:

The wide range of AWS cloud services, including computing, storage, and database services. AWS Systems Manager also underscores the systems aspect of AWS assets. It allows for automation of IT operations and management tasks across AWS services, enabling the management of the entire lifecycle of AWS resources. It integrates services like AWS CloudTrail and AWS Config to provide a unified view of system health and compliance.[xx]

e. Intellectual Property:

AWS's proprietary technologies, source code, and internal documentation.

f. Inherited Controls:

Controls which a customer fully inherits from AWS like Physical and Environmental controls

g. Shared Controls:

Controls which apply to both the infrastructure layer and customer layers, but in completely separate contexts or perspectives. In a shared control, AWS provides the requirements for the infrastructure and the customer must provide their own control implementation within their use of AWS services. Examples include:

- Patch Management – AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications.
- Configuration Management – AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.
- Awareness & Training - AWS trains AWS employees, but a customer must train their own employees.

h. Customer Specific Controls:

which are solely the responsibility of the customer based on the application they are deploying within AWS services. Examples include:

- Service and Communications Protection or Zone Security which may require a customer to route or zone data within specific security environments.

i. People:

While specific information on the role of people as assets within AWS wasn't directly found in the provided sources, AWS's emphasis on security, innovation, and customer service implicitly underscores the importance of skilled professionals in maintaining its operations, developing new services, and supporting customers' needs.

The table 1.01 highlights the impact score of all the AWS assets across different categories that we have classified it against to have a better overall understanding of the impact of each asset.

Category	AWS Assets	Impact Score
Core Services	Amazon S3 (Simple Storage Service)	90
Infrastructure Assets	Data centers	87
Infrastructure Assets	Servers	87
Data Assets	Databases	87
System assets	Applications	87
Inherited controls	Physical Security	87
Inherited controls	Network Infrastructure	87
Core Services	Amazon EC2 (Elastic Compute Cloud)	84
Inherited controls	Disaster Recovery Plan	84
Inherited controls	Compliance Certifications	83
Employees/People	Sales and Marketing Teams	79
Intellectual property	Custom Code	78
Core Services	Amazon RDS (Relational Database Service)	77
Infrastructure Assets	Availability Zones	77
Data Assets	Data Lakes	77
Data Assets	Backups	77
Inherited controls	Information Security Policies and Procedures	77
Employees/People	People in AWS organization	75
Intellectual property	Algorithms	74
Infrastructure Assets	Networking Hardware	71
Core Services	AWS Lambda	70
Employees/People	Legal and Compliance Staff	67
Core Services	AWS Identity and Access Management (IAM)	67

Employees/People	Customer Service and Support Teams	66
System assets	Operating Systems	65
System assets	Management Systems	65
Core Services	Amazon DynamoDB	64
Data Assets	Logs	64
Inherited controls	Environmental Controls	64
Core Services	Elastic Load Balancing	61
Intellectual property	Patents and Trademarks	60
Core Services	Amazon VPC (Virtual Private Cloud)	57
Data Assets	Machine Learning Models	57
Core Services	AWS cloudfront	55
Core Services	Amazon Route 53	55
Core Services	AWS Elastic Beanstalk	55
Core Services	Amazon Simple Notification Service (SNS) and Amazon Simple Queue Service (SQS)	55
Infrastructure Assets	Edge Locations	54
Infrastructure Assets	Direct Connect Locations	54
Infrastructure Assets	Submarine Cable Systems	54
Data Assets	Artifact Repositories	54
Intellectual property	Software Libraries and SDKs	53
System assets	Container Services	48
System assets	Development Tools	45
Employees/People	People outside AWS organization	44
Intellectual property	Educational Content	36

Table 1.01 – List of AWS Assets

5. Asset Impact Score

CATEGORY	AWS ASSETS	CONFIDENTIALITY	INTEGRITY/AVAILABILITY (IMPACT TO PROFITABILITY)	IMPACT ON REVENUE (weight=30)	IMPACT ON PROFITABILITY (weight=40)	IMPACT ON PUBLIC IMAGE (weight=30)	WEIGHTED SCORE
Core Services	Amazon S3 (Simple Storage Service)	Confidential	Critical	0.9	0.9	0.9	90
	Amazon EC2 (Elastic Compute Cloud)	Confidential	Critical	0.9	0.9	0.7	84
	Amazon RDS (Relational Database Service)	Confidential	Critical	0.8	0.8	0.7	77
	AWS Lambda	Confidential	Critical	0.75	0.7	0.65	70
	Amazon DynamoDB	Confidential	Critical	0.6	0.7	0.6	64
	Elastic Load Balancing	Internal	Critical	0.65	0.7	0.45	61
	Amazon VPC (Virtual Private Cloud)	Confidential	Critical	0.6	0.6	0.5	57
	AWS Identity and Access Management (IAM)	Internal	Critical	0.7	0.7	0.6	67
	AWS cloudfront	Internal	Critical	0.6	0.7	0.3	55
	Amazon Route 53	Internal	Critical	0.6	0.7	0.3	55
	AWS Elastic Beanstalk	Internal	Critical	0.6	0.7	0.3	55
	Amazon Simple Notification Service (SNS) and Amazon Simple Queue Service (SQS)	Internal	Critical	0.6	0.7	0.3	55
Infrastructure Assets	Data centers	Confidential	Critical	0.9	0.9	0.8	87
	Servers	Confidential	Critical	0.9	0.9	0.8	87
	Availability Zones	Confidential	Critical	0.8	0.8	0.7	77
	Networking Hardware	Confidential	Critical	0.7	0.8	0.6	71
	Edge Locations	Internal	Essential	0.6	0.6	0.4	54
	Direct Connect Locations	Internal	Essential	0.6	0.6	0.4	54
	Submarine Cable Systems	Internal	Essential	0.6	0.6	0.4	54
Data Assets Data and information managed and processed in the AWS environment.	Databases	Private	Critical	0.9	0.9	0.8	87
	Data Lakes	Private	Critical	0.8	0.8	0.7	77
	Backups	Private	Critical	0.8	0.8	0.7	77
	Logs	Private/Internal	Critical	0.7	0.7	0.5	64
	Machine Learning Models	Confidential	Essential	0.6	0.6	0.5	57
	Artifact Repositories	Confidential	Essential	0.6	0.6	0.4	54
System assets The software and systems running within the AWS environment.	Operating Systems	Internal	Critical	0.6	0.8	0.5	65
	Applications	Internal	Critical	0.9	0.9	0.8	87
	Management Systems	Internal	Critical	0.7	0.8	0.4	65
	Container Services	Internal	Essential	0.5	0.6	0.3	48
	Development Tools	Internal	Essential	0.4	0.6	0.3	45

Intellectual property	Custom Code	Confidential	Critical	0.8	0.9	0.6	78
	Algorithms	Confidential	Critical	0.7	0.8	0.7	74
	Patents and Trademarks	Confidential	Critical	0.6	0.6	0.6	60
	Software Libraries and SDKs	Internal	Essential	0.6	0.5	0.5	53
	Educational Content	Internal	Essential	0.3	0.3	0.5	36
Inherited controls	Physical Security	Internal	Critical	0.8	0.9	0.9	87
	Network Infrastructure	Internal	Critical	0.9	0.9	0.8	87
	Disaster Recovery Plan	Internal	Critical	0.8	0.9	0.8	84
	Compliance Certifications	Internal	Critical	0.8	0.8	0.9	83
	Information Security Policies and Procedures	Internal	Critical	0.7	0.8	0.8	77
	Environmental Controls	Internal	Critical	0.6	0.7	0.6	64
Employees/People	Sales and Marketing Teams	Internal	Essential	0.9	0.7	0.8	79
	People in AWS organization	Internal	Essential	0.8	0.9	0.5	75
	Legal and Compliance Staff	Internal	Essential	0.5	0.7	0.8	67
	Customer Service and Support Teams	Internal	Essential	0.7	0.6	0.7	66
	People outside AWS organization	Confidential	Essential	0.5	0.5	0.3	44

Table 1.02 – Asset Impact Score

In the above Table 1.02, The Assets are firstly grouped into their respective categories, then we use a classification like the Traffic Light Protocol to classify these assets into Categories such as Confidential, Internal, Essential and Private. We do so to understand the importance of protecting the asset in terms of overall risk. We then estimate the impact on revenue, impact on profitability as well as impact on public image and then give each of these categories a particular weight. We consider Impact on revenue as 30 weight, Impact on Profitability as 40, and Impact on Public Image as 30. We then multiply the weight with these scores to calculate a final asset impact score. This score tells us where an asset stands in an organizational point of view. We can then apply controls to the assets with highest impact score first and the least impact score assets can be considered at the end if our budget allows us to do so.

6. Compliance Frameworks

AWS has implemented a comprehensive risk and compliance program that encompasses all stages of service design and deployment. This program routinely conducts weekly reviews of operational metrics to identify and mitigate risks. Central to this program is a control environment built on automation controls, which aim to reduce human error in operational processes.

Additionally, AWS operates a Business Risk Management (BRM) program that collaborates with various AWS business units to give the AWS Board of Directors and senior leadership a complete overview of the primary risks within AWS. This program provides independent oversight of risk across different AWS functions, conducting risk assessments and monitoring that help identify and address potential risks.

The BRM program also plays a crucial role in risk remediation by reporting its findings to directors and vice presidents, thus aiding in informed decision-making across the company.

Regarding compliance, AWS adheres to several IT standards categorized under Certifications and Attestations; Laws, Regulations, and Privacy; and Alignments and Frameworks. These compliance efforts are validated by third-party independent auditors who provide certifications, audit reports, or attestations of compliance. While AWS manages these compliance frameworks, it is still up to the customers to ensure they meet any applicable laws, regulations, and privacy standards specific to their industry or function. These compliance guidelines help AWS and its customers maintain rigorous security and compliance standards tailored to specific operational needs.[xxi]

Certifications / Attestations:

Compliance certifications and attestations are assessed by a third-party, independent auditor and result in a certification, audit report, or attestation of compliance.

- C5
- CMMC
- Cyber Essentials Plus
- DoD SRG
- ENS High
- FedRAMP
- FINMA
- FIPS
- GSMA
- HDS
- IRAP
- ISMAP
- ISO 9001
- ISO 27001
- ISO 27017
- ISO 27018
- K-ISMS
- MTCS Tier 3
- OSPAR
- PCI DSS Level 1
- SOC 1
- SOC 2
- SOC 3
- TISAX

Laws / Regulations:

AWS customers remain responsible for complying with applicable compliance laws and regulations. In some cases, AWS offers functionality (such as security features), enablers, and legal agreements (such as the AWS Data Processing Agreement and Business Associate Addendum) to support customer compliance.

No formal certification is available to (or distributable by) a cloud service provider within these law and regulatory domains.

- CLOUD Act
- HIPAA
- IRS 1075
- ITAR
- SEC Rule 17a-4(f)
- VPAT / Section 508

Alignments / Frameworks:

Compliance alignments and frameworks include published security or compliance requirements for a specific purpose, such as a specific industry or function. AWS provides functionality (such as security features) and enablers (including compliance playbooks, mapping documents, and whitepapers) for these types of programs.

Requirements under specific alignments and frameworks may not be subject to certification or attestation; however, some alignments and frameworks are covered by other compliance programs.

- CJIS
- CSA
- EU-US Privacy Shield
- FinTech – Japan
- FISC
- FISMA
- G-Cloud
- GxP (FDA CFR 21 Part 11)
- HITRUST
- Medical Information Guidelines – Japan
- MPAA
- NISC – Japan
- NIST
- Uptime Institute Tiers

By privacy laws -

Americas

- Act respecting the sharing of certain health information – Quebec
- Argentina Data Privacy
- Brazil Data Privacy
- California Consumer Privacy Act (CCPA)
- FERPA
- Freedom of Information and Protection of Privacy Act (FOIPPA) – British Columbia
- Health Information Act (HIA) – Alberta
- Personal Health Information Act (NL PHIA) – Newfoundland and Labrador
- Personal Health Information Act (PHIA) – Nova Scotia
- Personal Health Information Privacy and Access Act (NB PHIPAA) – New Brunswick
- Personal Health Information Protection Act (PHIPA) – Ontario

Asia Pacific

- Australia Data Privacy
- Hong Kong Data Privacy
- India Data Privacy
- Indonesia Data Privacy
- Japan Data Privacy
- Korea Data Privacy
- Malaysia Data Privacy
- New Zealand Data Privacy
- Philippines Data Privacy
- Singapore Data Privacy
- Taiwan Data Privacy
- Thailand Data Privacy

Europe, Middle East & Africa

- Cloud Computing Compliance Controls Catalog (C5)
- Cloud Infrastructure Services Providers in Europe (CISPE)
- EU Data Protection
- EU-US Privacy Shield
- General Data Protection Regulation (GDPR)
- South Africa Data Privacy

7. List of Potential Vulnerabilities

We have identified a comprehensive list of vulnerabilities.

1. Misconfigured S3 buckets allowing public access.
2. Improperly Configured Access Control Lists (ACLs)
3. Inadequate Encryption
4. Misconfigured Bucket Policies
5. Lack of Monitoring and Logging
6. Unrestricted Cross-Origin Resource Sharing (CORS)
7. Overly Permissive IAM Roles
8. Poor Key Management
9. Unsecured API Endpoints
10. Excessive Data Retention
11. Malicious Payloads
12. Insecure Direct Object References (IDOR)
13. Inadequate Backup and Recovery Plans
14. Exposed Sensitive Data on EC2 instances
15. Phishing Attacks
16. Malware
17. Outdates softwares
18. Misconfigurations
19. Insecure Third-Party Software
20. Supply Chain Attacks
21. Natural Disasters
22. Human Error
23. Compliance Violation
24. Lack of awareness
25. Legal and geopolitical risks

The cybersecurity landscape is rife with challenges, and our AWS services are no exception. We have identified critical vulnerabilities such as misconfigured S3 buckets and inadequately managed IAM roles, each carrying the potential for unauthorized data exposure. Other significant threats include outdated software on EC2 instances, which could be exploited by malware, and operational weaknesses like insufficient disaster recovery measures. These vulnerabilities were prioritized based on their risk scores, which consider both the likelihood of occurrence and the severity of impact.

Table 1.03 to 1.7 mainly showcases the calculations of our **Probability vs Impact Score** for **each** vulnerabilities, for detailed analysis we can also refer to the controls spreadsheet attached along with this report.

CYBERSECURITY THREATS	Description	Probability	Asset Impact Score	Risk Score = Probability * Asset Impact Score - Risk mitigate by current controls + uncertainity about vulnerability
Data Breaches				
S3 Buckets	Misconfigured S3 buckets allowing public access.	0.9	90	81
	Improperly Configured Access Control Lists (ACLs)	0.8	90	72
	Inadequate Encryption	0.2	90	18
	Misconfigured Bucket Policies	0.6	90	54
	Lack of Monitoring and Logging	0.6	90	54
	Unrestricted Cross-Origin Resource Sharing (CORS)	0.3	90	27
	Overly Permissive IAM Roles	0.7	90	63
	Poor Key Management	0.4	90	36
	Unsecured API Endpoints	0.4	90	36
	Excessive Data Retention	0.7	90	63
ıbases(Amazon RDS, DynamoDB, EFS)	Containing sensitive or critical data vulnerable to breaches.	0.8	87	69.6
	Malicious Payloads	0.8	87	69.6
EC2 instances	If these instances store sensitive data that is exposed.	0.7	84	58.8
	Insecure APIs and Endpoints	0.5	76	38
Phishing Attacks (IAM)	Phishing attacks could target administrative users to gain their credentials.	0.6	67	40.2
Malwares	EC2 servers instances can be infected with malware if not properly secured.	0.6	84	50.4

Table 1.03 – Data Breach Vulnerabilities Impact Score

Software Vulnerabilities				
Outdated Software	Running outdated operating systems or applications.	0.6	65	39
Misconfigurations	Incorrectly configured permissions in IAM, Misconfigured S3 bucket access policies, Poorly configured networking assets settings (VPC's, Security groups)	0.5	84	42
Third-party Software	EC2 instances running third-party software that may not be secure.	0.4	84	33.6

Table 1.04 Software Vulnerabilities Impact Score

Operational Risks				
Supply Chain Attacks	AWS lambda and serverless functions use third-party dependencies libraries that might be compromised.	0.7	70	49
Natural Disasters	Regional service disruptions due to natural disasters.	0.2	87	17.4
Human Error	Mismanagement leading to data loss or unauthorized access.	0.8	75	60

Table 1.05 – Operational Risks Impact score

:ompliance and Regulatory Risks				
Compliance Violations	non-compliance fines and data sovereignty issues	0.8	83	66.4
Lack of Awareness	Lack of security awareness in cloud can lead to a lot of unecessary security vulnerabilities	0.3	75	22.5

Table 1.06 Compliance and Regulatory Impact Score

Legal and Geopolitical Risks				
	Geopolitical events causing an impact to critical business functionality	0.4	60	24

Table 1.07 Legal and Geopolitical Impact Score

Risk Rating	
1 to 30	Low
30 to 50	Moderate
50 to 70	Major
70 to 100	Severe

Table 1.08– Risk Rating

Table 1.08 represents the risk ratings of our vulnerabilities. Our main objective will be to find out controls for the vulnerability and risks associated with our high impact score assets. Therefore, it is crucial to identify assets first. The assets then need to be categorized to find out the threat actors of each category of assets. These threats are compared through every asset in that category and the list we get is a comprehensive vulnerability list. These vulnerabilities should be assigned an impact score according to which controls should be determined.

8. Categories of Controls

Controls are assorted into groups like Preventative, Detective, Forensic, and Audit, each serving a distinct purpose in the cybersecurity landscape. These controls, ranging from IAM role management to encryption and monitoring, form the bedrock of our defensive strategy against cyber threats.

Preventative Controls: Aimed at preventing security incidents before they occur.

Examples: Firewalls, antivirus software, encryption, security policies, access controls, multifactor authentication, security awareness training.

Detective Controls: Designed to detect and alert on potential security breaches.

Examples: Intrusion detection systems (IDS), log monitoring, anomaly detection systems, security information and event management (SIEM) systems.

Forensic Controls: The controls that we use to investigate a security incident.

Examples: Incident Response plans, forensic investigation tools, logs from AWS CloudTrail, Elastic load balancing and amazon s3 buckets.

Corrective Controls: Implemented to respond to and correct the impact of a security incident.

Examples: Patch management systems, incident response teams, backup and restore procedures.

Deterrent Controls: Intended to discourage security violations.

Examples: Security policies, legal penalties, and sanctions for violations.

Recovery Controls: Used to restore resources and capabilities after a security breach.

Examples: Disaster recovery plans, database replication, server redundancy.

Physical Controls: Concerned with physically securing the enterprise environment.

Examples: Security guards, locks, biometric systems, surveillance cameras.

Technical Controls: Technological tools and solutions used to protect assets.

Examples: Encryption, smart cards, network filters, secure coding practices.

Administrative Controls: Management policies and procedures to control user behavior.

Examples: Security training and awareness programs, background checks, access authorization procedures.

Compensatory Controls: Alternative controls used when primary controls are not feasible.

Examples: Manual data review in place of automated scanning, temporary policies during an emergency.

Audit Controls: Processes that ensure compliance with policies and procedures and are used to detect anomalies.

Examples: Audit logs, accountability trails, periodic security reviews.

9. List of Controls

List of Tools Required for AWS Security Controls

Security and Monitoring Tools

AWS Config - Configuration management and compliance monitoring.

AWS CloudTrail - Governance, compliance, operational auditing, and risk auditing of AWS accounts.

AWS CloudWatch - Monitoring and observability of AWS resources and applications.

AWS KMS (Key Management Service) - Managed service to create and control encryption keys.

AWS Inspector - Automated security assessment service to help improve the security and compliance of applications deployed on AWS.

AWS WAF (Web Application Firewall) - Protects web applications from common web exploits.

AWS Systems Manager - View and control your infrastructure on AWS.

AWS API Gateway - Create, publish, maintain, monitor, and secure APIs at any scale.

AWS Trusted Advisor - Provides real-time guidance to help you provision your resources following AWS best practices.

Third-party Security Tools

SIEM Tools (e.g., Splunk, IBM QRadar) - Security Information and Event Management for real-time analysis and logging of security alerts.

Database Monitoring Tools - For monitoring real-time database performance and security.

Phishing Detection Software - Tools to detect and prevent phishing attacks, such as Proofpoint or Mimecast.

Email Filtering Solutions - Advanced solutions for filtering spam and malicious emails.

Vulnerability Scanning Tools - Tools to identify security vulnerabilities in applications, such as Qualys or Nessus.

Patch Management Software - Automates the patch management process for maintaining system updates.

Network Security Tools - Tools to secure network traffic and protect against intrusions.

Secure Software Development Tools - Tools that support secure coding practices and review code for vulnerabilities.

Geopolitical Monitoring Tools - Tools to monitor and report on geopolitical events that might impact data governance.

List of Security Positions at Amazon to Implement These Controls

Core Security Positions

Security Engineers - Implement and manage security tools, conduct security reviews, and address security issues.

Cloud Security Architect - Design and review the architecture of AWS deployments from a security perspective.

Security Analysts - Monitor security systems for events and incidents, and respond to security breaches.

Compliance Officers - Ensure compliance with regulatory requirements and internal security policies.

IT Security Manager - Oversee the IT security strategy and the team of security professionals.

Data Protection Officer - Manage data protection strategies, compliance, and privacy laws.

Specialized Security Positions

Forensic Analysts - Investigate and analyze breaches to determine the root cause and the extent of the impact.

Penetration Testers - Perform simulated attacks to identify and fix vulnerabilities.

Security Operations Center (SOC) Analysts - Operate in the SOC to monitor and react to real-time security threats.

Incident Response Managers - Manage the response to security incidents and breaches.

Security Awareness Trainer - Develop and deliver security training programs for staff to prevent human errors and breaches.

Legal and Compliance Analyst - Focus on compliance with laws and regulations, particularly in different jurisdictions for multinational operations.

These tools and positions are essential to create a robust security infrastructure in AWS environments, addressing various security and compliance requirements effectively. For

Amazon, leveraging these resources ensures that its vast cloud infrastructure and services remain secure and compliant with global standards.

10. Cost of Controls

Our controls are ranked based on their impact and the severity of the risks they mitigate. At the top are measures addressing misconfigurations in S3 buckets, followed by encryption enforcement for databases. User education and robust access controls form the next line of defence, particularly against phishing and malware. This prioritization ensures that the most impactful measures are implemented swiftly, offering the greatest return on investment in terms of risk reduction. The costs are approximating to the best of our knowledge and not exact values publicly disclosed by the organization.

Control Category	Tools/Services	Details	Annual Cost
Data Breaches - S3 Buckets	AWS Config	Configuration monitoring and management	$150,000
	AWS CloudTrail and CloudWatch	Logging and real-time monitoring	$200,000
	S3 Encryption Tools	At-rest and in-transit encryption	$50,000
	SIEM Tools	Security information and event management	$300,000
	Policy Validation Tools	Access and permissions management	$100,000
Database Vulnerabilities	AWS KMS	Key management service for encryption	$70,000
	AWS Inspector	Automated security assessment service	$150,000
	Database Monitoring Tools	Real-time database monitoring	$120,000
	Vulnerability Scanning Tools	Regular vulnerability scans	$100,000
Compliance & Regulatory	AWS Config	Compliance tracking across resources	$150,000
	AWS Trusted Advisor	Best practice checks and recommendations	$100,000
	Compliance Management Software	Manage, track, and report on compliance	$200,000
	Audit Management Tools	Tools to facilitate and manage audits	$110,000
Operational - Human Error	Error Tracking Software	Track and analyze human error incidents	$60,000
	Audit Management Software	Support for policy and operation reviews	$60,000
	Training Tools	Tools for staff training on error prevention	$40,000
EC2 Instances - Malware	AWS Systems Manager	System operations and patch management	$100,000
	AWS Inspector	Security assessments for EC2 instances	$150,000
	Anti-Malware Tools	Malware protection for EC2 instances	$150,000
	Security Configuration Tools	Tools to enforce and manage security settings	$110,000
Supply Chain Attacks	AWS CodePipeline and CodeSign	Secure code delivery and integrity verification	$140,000
	Secure Software Development Tools	Tools to secure software development lifecycle	$160,000
Misconfigurations	AWS Config	Monitoring and correcting configurations	$100,000
	Configuration Compliance Software	Ensure compliance with security standards	$80,000
Phishing Attacks	AWS WorkMail	Managed email service with security features	$25,000
	Phishing Detection Software	Tools to detect and prevent phishing attacks	$100,000
	Email Filtering Solutions	Advanced filtering to block malicious emails	$75,000
Software Vulnerabilities - Outdated Software	AWS Systems Manager	Automated patching and updates	$80,000
	Patch Management Software	Tools to manage and deploy patches	$70,000
	Vulnerability Scanning Software	Continuous scanning for software vulnerabilities	$100,000
Third-party Software Attacks	AWS API Gateway and WAF	API management and web application firewall	$160,000
	Network Security Tools	Enhance security across third-party applications	$100,000
Legal and Geopolitical Issues	AWS CloudTrail	Governance and compliance logging	$40,000
	Geopolitical Monitoring Tools	Tools to monitor and respond to geopolitical changes	$50,000

Table 1.10 – Cost of Controls

Our analysis of cost calculation in the table 1.10 showcase the cost behind implementing these controls. These controls will significantly mitigate risks, potentially reducing our vulnerability by up to 80%. However, this is not a set-and-forget scenario – continual vigilance and updating of these controls are mandatory to keep pace with the dynamic nature of cyber threats.

11. Budget Profile

Crafting a cybersecurity budget is a strategic initiative critical to the digital fortification of an enterprise. It requires a nuanced approach that aligns with the organization's overarching mission and operational scale. The intent is to construct a financial shield that is both cost-effective and maximally protective, ensuring the integrity of the enterprise's assets against potential security breaches. In the landscape of enterprise security, budgeting transcends mere number-crunching; it is about understanding risk profiles, prioritizing assets, and leveraging a robust security posture to prevent breaches that could undermine the enterprise's credibility and financial standing. The challenge lies in assessing the impacts of cybersecurity initiatives on organizational resilience and translating these into quantifiable financial commitments.

A methodical strategy to budget development is through a systematized approach that reflects the organizational hierarchy, where security initiatives are prioritized based on their criticality and interdependencies. This approach is reflective of a 'systems thinking' methodology where 'child' tasks support 'parent' operations. For instance, strengthening authentication processes underpins broader access control measures, laying the groundwork for comprehensive risk mitigation. Defining strategic goals upfront is vital in directing the cybersecurity budget. Objectives may range from minimizing attack surfaces, neutralizing threats to swift recovery from security incidents, all aimed at minimizing downtime and preserving business continuity. The endgame is to cultivate an agile cyber defense ecosystem capable of not just defending against but also anticipating and countering cyber threats.

The construction of the cybersecurity budget is predicated upon the identified control mechanisms pertinent to the enterprise's unique vulnerabilities. Fundamental to this construction are the human capital—experts who architect, implement, and maintain cybersecurity measures—and the arsenal of tools and technologies they employ, all underpinned by efficient processes and stringent policies. We advocate for a tiered budgeting framework, tailored to different investment levels:

Minimal Cost Budget: Focuses on the most pressing risks with a keen eye on cost-efficiency.

Practical Cost Budget: Aims for a balanced approach, managing risks to maintain 'reasonable' residual risk.

Money-no-object Budget: Allocates extensive resources to cover all possible threats comprehensively.

In the context of an enterprise, the pivotal consideration is the alignment of the cybersecurity budget with business objectives, ensuring that every dollar spent contributes to the safeguarding of critical assets and the seamless operation of business processes. A dynamic and forward-looking cybersecurity budget is not merely a fiscal plan; it is a manifestation of the enterprise's commitment to safeguarding its digital ecosystem in an ever-evolving threat landscape.

12. Categorization of Budget

Within the cybersecurity budget framework, initial setup costs are encapsulated within the broader financial allocation for AWS tools and services, as well as third-party tools. These initial costs are foundational investments, paving the way for the deployment and operationalization of the security infrastructure. The people cost is another crucial component, encompassing not only the salaries of dedicated security personnel but also the investment in their development through comprehensive training programs. This training ensures that the team remains adept at utilizing the full spectrum of tools at their disposal, maintaining the organization's resilience against cybersecurity threats. It's a strategic infusion of capital designed to empower the human element of our cybersecurity defense, which is as pivotal as the technological components themselves. The table 1.11 describes the cost description for individual components of our security Budget.

Components	Cost Description
Personnel Costs	Annual salaries for security personnel
AWS Tools & Service Costs	Annual costs for using AWS tools and services
Third-party Tool Costs	Annual costs for additional non-AWS security tools
Policy Cost	Cost for Continuously updating and maintaining policies
Training & Licenses	Costs for training and certification of personnel
Research & Miscellaneous Costs	Any other related expenses
Total First Year Costs	Sum of all the above for the first year

Table 1.11 – Components vs Cost Description

Personnel Costs: This segment encompasses the annual compensation for cybersecurity professionals employed by Amazon Web Services. Salary estimations are grounded on the prevailing market rates reported on employment and salary databases such as Glassdoor. These figures are formulated by examining the average hourly wages for each role and extrapolating to annual compensation considering a standard work year.

AWS Tools & Service Costs: These are the aggregate costs incurred from the utilization of AWS-specific tools and services over the year. AWS provides a comprehensive list of pricing for its services, which can be leveraged to forecast this aspect of the budget.

Third-party Tool Costs: This line item tallies the annual expenditure on security tools that are external to the AWS ecosystem. It includes costs associated with licenses, subscriptions, or purchases of supplementary cybersecurity software and services that bolster the security measures provided by AWS.

Policy Cost: This accounts for the resources dedicated to the continuous development, revision, and enforcement of cybersecurity policies. It includes the administrative overhead and the professional hours

spent in policy management to ensure they stay updated with the latest compliance regulations and industry best practices.

Training & Licenses: This portion of the budget is allocated for the training and continuous education of the cybersecurity workforce, as well as for the costs related to obtaining and maintaining professional certifications. This ensures that personnel are up-to-date with the latest security skills and knowledge.

Research & Miscellaneous Costs: This broad category includes all other related expenses not captured in the previous sections. It can cover a range of items, from academic research collaborations to investments in emerging technology assessments and exploratory projects aimed at enhancing AWS's security posture.

Total First Year Costs: Represents the aggregate of all the costs, yielding the complete financial outlook for the initial year of the cybersecurity budget implementation.

a. Low-Cost Budget

The Low-cost budget effectively allocates resources across a broad spectrum of controls, ensuring that each control covers the most critical risks and is not just a theoretical measure but is actively supported by qualified professionals and the necessary technological tools. The emphasis on AWS Config, CloudTrail, CloudWatch, and the AWS WAF signifies a robust defense mechanism for monitoring, logging, and protecting web applications. Third-party tools such as SIEM, database monitoring, and vulnerability scanning tools are pivotal for a layered security approach, extending protection beyond the AWS suite's capabilities.

Resources	Roles/Items	Quantity	Hourly Rate	Required Hours/Week	Weekly Costs	Monthly Costs	PTO Hrs/Year	Per Employee Cost	Total Annual Cost
People	CISO	1	88.54	40	3,541.67	14,166.67	80.00	1,77,083.33	USD 1,77,083.33
	Security Engineers	1	59.10	40	2,364.19	9,456.75	80.00	1,18,209.38	USD 1,18,209.38
	Cloud Security Architect	1	90.70	40	3,627.85	14,511.42	80.00	1,81,392.71	USD 1,81,392.71
	Security Analysts	2	56.29	40	4,503.33	18,013.33	80.00	4,41,326.67	USD 4,41,326.67
	Compliance Officers	1	52.08	40	2,083.33	8,333.33	80.00	1,04,166.67	USD 1,04,166.67
	IT Security Manager	1	72.92	40	2,916.67	11,666.67	80.00	1,45,833.33	USD 1,45,833.33
	Penetration Testers	1	62.50	40	2,500.00	10,000.00	80.00	1,25,000.00	USD 1,25,000.00
	SOC Analysts	2	52.08	40	4,166.67	16,666.67	80.00	4,08,333.33	USD 4,08,333.33
	Incident Response Managers	1	62.50	40	2,500.00	10,000.00	80.00	1,25,000.00	USD 1,25,000.00
	Legal and Compliance Analysts	1	57.29	40	2,291.67	9,166.67	80.00	1,14,583.33	USD 1,14,583.33
AWS Tools and Services	AWS Config	1						USD 1,50,000.00	USD 1,50,000.00
	AWS CloudTrail	1						USD 2,00,000.00	USD 2,00,000.00
	AWS CloudWatch	1						USD 1,00,000.00	USD 1,00,000.00
	AWS WAF (Web Application Firewall)	1						USD 1,30,000.00	USD 1,30,000.00
	AWS Systems Manager	1						USD 75,000.00	USD 75,000.00
	AWS API Gateway	1						USD 1,00,000.00	USD 1,00,000.00
Third-party Security Tools	SIEM Tools (e.g., Splunk, IBM QRadar)	1						USD 3,00,000.00	USD 3,00,000.00
	Database Monitoring Tools	1						USD 1,80,000.00	USD 1,80,000.00
	Phishing Detection Software (e.g., Proofpoint, Mimecast)	1						USD 1,50,000.00	USD 1,50,000.00
	Email Filtering Solutions	1						USD 1,20,000.00	USD 1,20,000.00
	Vulnerability Scanning Tools (e.g., Qualys, Nessus)	1						USD 2,00,000.00	USD 2,00,000.00
	Patch Management Software	1						USD 1,00,000.00	USD 1,00,000.00
	Network Security Tools	1						USD 2,50,000.00	USD 2,50,000.00
	Secure Software Development Tools	1						USD 1,50,000.00	USD 1,50,000.00
Security Research									USD 5,00,000.00
								Total Personnel Cost	USD 22,05,000.00
								Total Tools Cost	USD 19,40,928.75
								Total Research Cost	USD 5,00,000.00
								Total Policy Cost	USD 0.00
								Total Training Cost	USD 0.00
								Total Annual Cost	**USD 46,45,928.75**

Table 1.12 – Low-cost Budget

The Low-Cost Security Budget, as visualized in Figure 1.09, presents a distribution where the majority of the allocation goes towards Personnel Costs at 47% and Tools Cost at 42%. This reflects a strategic focus on investing in skilled cybersecurity professionals and the necessary tools they require to protect the organization's digital assets effectively. The Security Research Cost accounts for 11% of the budget, underscoring the organization's commitment to staying ahead of the latest threats and vulnerabilities through ongoing research.

In this scenario, with a total security budget of $4,645,928 as seen in Table 1.12 and a workforce of 13,600 employees[xxii], the annual cost of security per employee would be calculated as follows:

Annual security cost per employee = Total security budget/ Number of employees = 34.16$ which is not bad for our low-cost security budget.

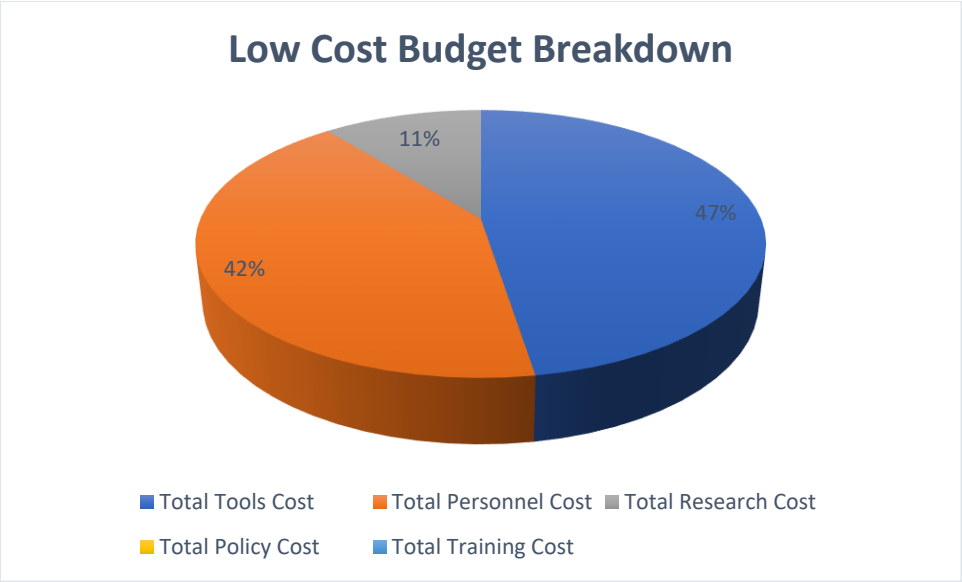

Fig. 1.09 – Low-cost Budget Breakdown

b. Practical Cost Budget

The detailed breakdown of the practical cost budget is described in the table 1.5 below. In the "Practical Cost Budget Breakdown" (Fig. 1.10), we see a significant proportion of the budget allocated to personnel costs, which makes up 75% of the total expenditures. This underlines the importance of skilled professionals in maintaining a robust security posture. Tools are the next significant investment at 16%, showcasing the reliance on sophisticated software and systems to safeguard assets. Research costs represent 6% of the budget, highlighting the continuous need for advancement and staying ahead of emerging threats. Policy and training each account for a smaller slice of the pie, at 2% and 1% respectively, but are critical for ensuring that the protocols and the workforce are up to date with the latest security practices.

As per our calculations in Table 1.13 With 13,600 employees at AWS, the annual per-person security cost under this budget would be approximately $118.96, derived from the total security budget of $16,177,962.25. This figure suggests a substantial investment in security per capita, emphasizing the organization’s commitment to protecting its assets, employees, and customers from potential cyber threats. This also reflects the enterprise's proactive stance on cybersecurity, opting to invest in comprehensive training, policy development, and state-of-the-art tools and services to bolster its defences.

Resources	Roles/Items	Quantity	Hourly Rate	Required Hours/Week	Weekly Costs	Monthly Costs	PTO Hrs/Year	Per Employee Cost	Total Annual Cost
People	CISO	1	88.54	40	3,541.67	14,166.67	80.00	1,77,083.33	USD 1,77,083.33
	Security Engineers	4	59.10	40	9,456.75	37,827.00	80.00	18,34,609.50	USD 18,34,609.50
	Cloud Security Architect	2	90.70	40	7,255.71	29,022.83	80.00	7,11,059.42	USD 7,11,059.42
	Security Analysts	4	56.29	40	9,006.67	36,026.67	80.00	17,47,293.33	USD 17,47,293.33
	Compliance Officers	2	52.08	40	4,166.67	16,666.67	80.00	4,08,333.33	USD 4,08,333.33
	IT Security Manager	2	72.92	40	5,833.33	23,333.33	80.00	5,71,666.67	USD 5,71,666.67
	Data Protection Officer	1	62.50	40	2,500.00	10,000.00	80.00	1,25,000.00	USD 1,25,000.00
	Forensic Analysts	4	52.08	40	8,333.33	33,333.33	80.00	16,16,666.67	USD 16,16,666.67
	Penetration Testers	5	62.50	40	12,500.00	50,000.00	80.00	30,25,000.00	USD 30,25,000.00
	SOC Analysts	3	52.08	40	6,250.00	25,000.00	80.00	9,12,500.00	USD 9,12,500.00
	Incident Response Managers	2	62.50	40	5,000.00	20,000.00	80.00	4,90,000.00	USD 4,90,000.00
	Security Awareness Trainers	1	57.29	40	2,291.67	9,166.67	80.00	1,14,583.33	USD 1,14,583.33
	Legal and Compliance Analysts	2	57.29	40	4,583.33	18,333.33	80.00	4,49,166.67	USD 4,49,166.67
AWS Tools and Services	AWS Config	1						USD 1,50,000.00	USD 1,50,000.00
	AWS CloudTrail	1						USD 2,00,000.00	USD 2,00,000.00
	AWS CloudWatch	1						USD 1,00,000.00	USD 1,00,000.00
	AWS KMS (Key Management Service)	1						USD 80,000.00	USD 80,000.00
	AWS Inspector	1						USD 1,20,000.00	USD 1,20,000.00
	AWS WAF (Web Application Firewall)	1						USD 1,30,000.00	USD 1,30,000.00
	AWS Systems Manager	1						USD 75,000.00	USD 75,000.00
	AWS API Gateway	1						USD 1,00,000.00	USD 1,00,000.00
	AWS Trusted Advisor	1						USD 90,000.00	USD 90,000.00
Third-party Security Tools	SIEM Tools (e.g., Splunk, IBM QRadar)	1						USD 3,00,000.00	USD 3,00,000.00
	Database Monitoring Tools	1						USD 1,80,000.00	USD 1,80,000.00
	Phishing Detection Software (e.g., Proofpoint, Mimecast)	1						USD 1,50,000.00	USD 1,50,000.00
	Email Filtering Solutions	1						USD 1,20,000.00	USD 1,20,000.00
	Vulnerability Scanning Tools (e.g., Qualys, Nessus)	1						USD 2,00,000.00	USD 2,00,000.00
	Patch Management Software	1						USD 1,00,000.00	USD 1,00,000.00
	Network Security Tools	1						USD 2,50,000.00	USD 2,50,000.00
	Secure Software Development Tools	1						USD 1,50,000.00	USD 1,50,000.00
Security Research									USD 10,00,000.00
Security Training									USD 3,00,000.00
Compliance									USD 2,00,000.00
Policy									USD 2,00,000.00
								Total Tools Cost	USD 24,95,000.00
								Total Personnel Cost	USD 1,21,82,962.25
								Total Research Cost	USD 10,00,000.00
								Total Policy Cost	USD 2,00,000.00
								Total Training Cost	USD 3,00,000.00
								Total Annual Cost	**USD 1,61,77,962.25**

Table 1.13 – Practical Cost Budget

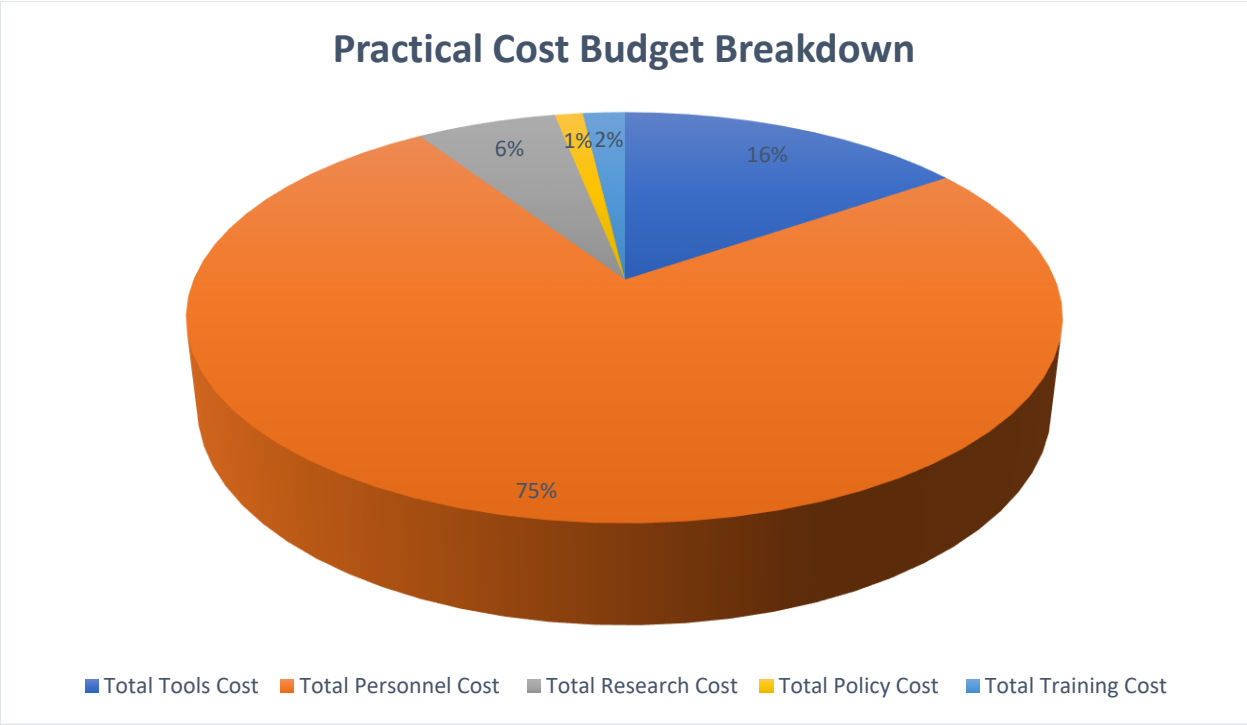

Fig. 1.10 Practical Cost Budget Breakdown

c. Money Not an Object Budget

The pie chart labelled "Money Not an Object Budget" depicts a budget distribution where the vast majority of expenses, 79%, are allocated to Total Personnel Costs. This substantial portion reflects the emphasis on skilled labour, suggesting that a significant investment is made in hiring, training, and retaining top-tier security personnel, which is essential for the effective implementation of cybersecurity measures. Total Tools Cost constitutes 12% of the budget, indicating a strong commitment to acquiring advanced tools and services for comprehensive security management. The 7% allocated to Total Research Cost signifies a dedication to ongoing security innovations and staying ahead of evolving threats. Total Policy Cost and Total Training Cost, each at 1%, while smaller, are critical components that ensure policies are current and personnel are well-informed about the latest security protocols and threats. Table 1.6 shows the detailed breakdown of the Budget.

As per Fig. 1.11, the total security budget of USD 376,002,225.00, when divided among the 13,600 employees working across various departments at AWS, results in an annual security expenditure of USD 276.47 per person. This figure underscores the organization's substantial investment in securing its operations and personnel, underpinning the high priority placed on cybersecurity within the company's operational budget. Table 1.14 showcase the cost calculations for our High security Budget.

Cybersecurity Insurance: While not listed, investing in cybersecurity insurance could be a safety net to mitigate financial losses from potential cyber incidents that exceed the scope of preventive measures.

Resources	Roles/Items	Quantity	Hourly Rate	Required Hours/Week	Weekly Costs	Monthly Costs	PTO Hrs/Year	Per Employee Cost	Total Annual Cost
People	CISO	1	88.54	40	3,541.67	14,166.67	80.00	1,77,083.33	USD 1,77,083.33
	Security Engineers	8	59.10	40	18,913.50	75,654.00	80.00	73,00,611.00	USD 73,00,611.00
	Cloud Security Architect	4	90.70	40	14,511.42	58,045.67	80.00	28,15,214.83	USD 28,15,214.83
	Security Analysts	8	56.29	40	18,013.33	72,053.33	80.00	69,53,146.67	USD 69,53,146.67
	Compliance Officers	2	52.08	40	4,166.67	16,666.67	80.00	4,08,333.33	USD 4,08,333.33
	IT Security Manager	2	72.92	40	5,833.33	23,333.33	80.00	5,71,666.67	USD 5,71,666.67
	Data Protection Officer	2	62.50	40	5,000.00	20,000.00	80.00	4,90,000.00	USD 4,90,000.00
	Forensic Analysts	5	52.08	40	10,416.67	41,666.67	80.00	25,20,833.33	USD 25,20,833.33
	Penetration Testers	5	62.50	40	12,500.00	50,000.00	80.00	30,25,000.00	USD 30,25,000.00
	SOC Analysts	5	52.08	40	10,416.67	41,666.67	80.00	25,20,833.33	USD 25,20,833.33
	Incident Response Managers	2	62.50	40	5,000.00	20,000.00	80.00	4,90,000.00	USD 4,90,000.00
	Security Awareness Trainers	2	57.29	40	4,583.33	18,333.33	80.00	4,49,166.67	USD 4,49,166.67
	Legal and Compliance Analysts	4	57.29	40	9,166.67	36,666.67	80.00	17,78,333.33	USD 17,78,333.33
AWS Tools and Services	AWS Config	1						USD 1,50,000.00	USD 1,50,000.00
	AWS CloudTrail	1						USD 2,00,000.00	USD 2,00,000.00
	AWS CloudWatch	1						USD 1,00,000.00	USD 1,00,000.00
	AWS KMS (Key Management Service)	1						USD 80,000.00	USD 80,000.00
	AWS Inspector	1						USD 1,20,000.00	USD 1,20,000.00
	AWS WAF (Web Application Firewall)	1						USD 1,30,000.00	USD 1,30,000.00
	AWS Systems Manager	1						USD 75,000.00	USD 75,000.00
	AWS API Gateway	1						USD 1,00,000.00	USD 1,00,000.00
	AWS WorkMail	1						USD 25,000.00	USD 25,000.00
	AWS Trusted Advisor	1						USD 90,000.00	USD 90,000.00
Third-party Security Tools	SIEM Tools (e.g., Splunk, IBM QRadar)	2						USD 3,00,000.00	USD 6,00,000.00
	Database Monitoring Tools	2						USD 1,80,000.00	USD 3,60,000.00
	Phishing Detection Software (e.g., Proofpoint, Mimecast)	2						USD 1,50,000.00	USD 3,00,000.00
	Email Filtering Solutions	1						USD 1,20,000.00	USD 1,20,000.00
	Vulnerability Scanning Tools (e.g., Qualys, Nessus)	5						USD 2,00,000.00	USD 10,00,000.00
	Patch Management Software	2						USD 1,00,000.00	USD 2,00,000.00
	Network Security Tools	2						USD 2,50,000.00	USD 5,00,000.00
	Secure Software Development Tools	2						USD 1,50,000.00	USD 3,00,000.00
	Geopolitical Monitoring Tools	2						USD 75,000.00	USD 1,50,000.00
Security Research									USD 25,00,000.00
Security Training									USD 5,00,000.00
Compliance									USD 5,00,000.00
Policy									USD 5,00,000.00
								Total Tools Cost	USD 46,00,000.00
								Total Personnel Cost	USD 2,95,00,222.50
								Total Research Cost	USD 25,00,000.00
								Total Policy Cost	USD 5,00,000.00
								Total Training Cost	USD 5,00,000.00
								Total Annual Cost	**USD 3,76,00,222.50**

Table 1.14 – Money Not an Object Budget

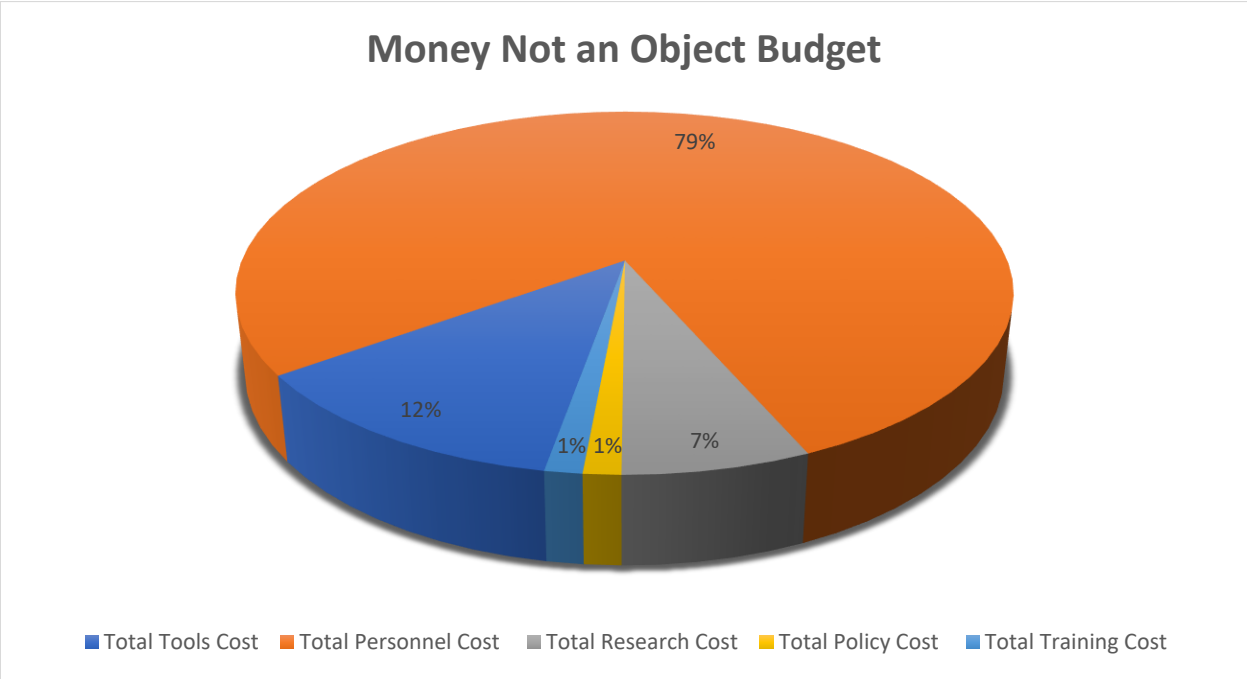

Fig 1.11 – Money Not an Object Budget Breakdown

13. Company Values vs Company Needs

When comparing the needs of AWS in terms of cybersecurity to the overall value of the company, it's important to consider how closely intertwined AWS's operational integrity and customer trust are with its cybersecurity posture. AWS, as a leading cloud service provider, handles vast amounts of sensitive data and provides infrastructure critical to businesses around the world. The company's value is deeply rooted in its reliability, security, and ability to innovate—attributes that are directly impacted by its approach to cybersecurity.

1. Operational Needs vs. Market Value

AWS's operational needs for cybersecurity are vast and complex due to its global scale and the nature of its services. The company operates data centers around the world and offers a wide range of services that require robust protection against a variety of cyber threats, including data breaches, denial of service attacks, and more sophisticated targeted attacks. The need for strong cybersecurity measures is critical not just for protecting operational infrastructure but also for maintaining business continuity and compliance with global regulatory requirements. The value of AWS to its customers lies in its ability to provide secure, reliable, and scalable cloud services. A significant breach or a series of smaller breaches could undermine customer trust, leading to loss of business and potentially severe financial repercussions. Given that AWS accounted for a substantial portion of Amazon's operating profits, the value of maintaining an impeccable security record extends beyond operational integrity to include shareholder value and market position.

2. Financial Investment in Cybersecurity vs. Financial Health

The financial investment in cybersecurity needs to be viewed as a mechanism to protect and potentially increase the company's market value. AWS's investment in cybersecurity is not merely an operational expense but a strategic investment that directly contributes to sustaining its competitive advantage and market leadership. By comparing the costs associated with implementing and maintaining robust cybersecurity measures with the potential costs of security breaches (including direct financial losses, regulatory fines, and reputational damage), it becomes evident that proactive investment in cybersecurity safeguards the larger financial health and ongoing value proposition of the company.

3. Long-term Value Preservation vs. Short-term Costs

In the long term, the costs of robust cybersecurity measures are far outweighed by the benefits they provide in maintaining customer trust and compliance with increasingly strict regulatory landscapes. As businesses increasingly rely on cloud infrastructure for critical operations, AWS's commitment to security becomes a key determinant of its value proposition. Investing in advanced security technologies, skilled personnel, and comprehensive risk management strategies not only addresses immediate operational needs but also positions AWS as a leader in a sector where security is a primary concern for customers.

In conclusion, the cybersecurity needs of AWS are directly aligned with its core value propositions of reliability, trust, and service excellence. Strategic investments in cybersecurity not only protect but can

enhance the company's value by ensuring it remains a trusted, compliant, and competitive service provider in the rapidly evolving digital landscape.

14. Analysis of Controls

This section provides a detailed breakdown of AWS's cybersecurity spending. The financial analysis includes direct costs associated with implementing specific security measures and the administrative overheads related to managing these security processes.

Expenditure Per Employee: AWS spends an estimated $276.47 per employee on cybersecurity annually where the security budget is calculated with money as no object. This figure is derived from the total security budget divided by the number of AWS employees, highlighting the per capita investment in protecting company assets. We have also rated each controls based on their overall standing in table 1.09 below.

Total Overall Costs: The total cybersecurity budget for AWS is segmented into low, practical, and high-cost scenarios, reflecting different levels of investment and corresponding levels of risk mitigation:

Low-Cost Budget: $4,645,928 focused on essential security measures.

Practical Cost Budget: $16,177,962, which balances cost and comprehensive risk management.

High-Cost Budget: $376,002,225, aimed at extensive coverage and minimal residual risk.

The comparison also covers how AWS's spending on cybersecurity compares to industry averages and the best practices of leading competitors.

GRAPH comparing AWS SECURITY ESTIMATE TO AVERAGE SPENDINGS

a. Most effective controls

AWS has strategically implemented a range of preventive controls that are classified as most effective in mitigating risks associated with enterprise-related vulnerabilities. These controls are critical and strongly recommended for maintaining business continuity and safeguarding against potential threats. Specific effective controls include Identity and Access Management (IAM) policies, which restrict access to only authorized users, and encryption protocols for data at rest and in transit, ensuring data integrity and confidentiality. Additionally, network segmentation effectively isolates sections of the network, limiting the spread of potential intrusions. These measures are constantly evaluated and enhanced to counter new threats, forming a resilient and dynamic defense mechanism within AWS’s cybersecurity infrastructure.

b. Highly Effective Controls

In the realm of detective controls, AWS leverages advanced threat detection systems like Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) systems, which are deemed highly effective. These systems play a crucial role in the early detection of threats within the cyber kill chain, thereby enhancing AWS's ability to preemptively address potential security incidents. The real-time monitoring and logging capabilities of these tools allow for swift identification and mitigation of threats, integral to maintaining AWS's robust security posture. Regular security audits and compliance checks further reinforce these systems, ensuring alignment with industry standards and enhancing the overall security framework.

c. Least Effective Controls

The table identifies forensic and audit controls as less effective compared to preventive and detective controls. Forensic controls, while severe in their necessity for post-incident investigations, are inherently reactive and thus less effective in preventing incidents before they occur. These controls are crucial for understanding and mitigating the aftermath of security incidents but fall short in initial prevention. Similarly, audit controls, classified as moderate in effectiveness, are essential for ensuring compliance and detecting anomalies but do not directly prevent security breaches. AWS is actively working to enhance these controls, integrating them with more proactive measures to evolve its defense strategies in line with emerging cybersecurity challenges.

Vulnerabilities	Controls			
	Preventative	Detective	Forensic	Audit
Enterprise Related Vulnerabilities	Critical; Strongly recommended	Severe; Helps detect threats at an early stage in the cyber kill chain; Helps in business continuity	Moderate	Moderate
AWS Product based Vulnerabilities	Critical; Hard/Costly to implement but required	Critical; Hard to detect technology threats with evolving threat landscape; High Initial Costs	Severe	Moderate

Table 1.09 Controls in the Big Picture

Strategic Recommendations

Based on the analysis conducted, several strategic recommendations can be made to enhance AWS's cybersecurity posture:

Strengthen Forensic Capabilities: Given that forensic controls are identified as a weaker aspect of AWS's cybersecurity framework, it is recommended to invest in advanced forensic tools and training for security teams to improve incident response and post-breach analyses.

Expand Endpoint Detection: Increase investment in endpoint detection and response (EDR) solutions to better monitor and respond to threats at the device level, particularly for remote employees and IoT devices.

Enhance Encryption Practices: Given the critical nature of data privacy, enhancing encryption across all data storage and transmission points will help mitigate risks associated with data breaches and unauthorized access.

Implement Advanced AI and Machine Learning: Utilize more advanced artificial intelligence and machine learning algorithms to predict and pre-emptively counteract potential security threats before they can impact AWS services.

Normalization of Security Measures

AWS has implemented a wide range of security measures across its global operations to ensure consistency and effectiveness in its cybersecurity protocols. This section describes how AWS normalizes these security measures to maintain a uniform security posture across all regions and services. The company utilizes a centralized policy framework that dictates the security configurations and procedures to be followed for every AWS service. These policies are enforced through automated systems that ensure compliance and uniformity.

To handle specific regional compliance requirements, AWS incorporates local regulations into its global security model, customizing only where necessary while maintaining core security principles. For example, data sovereignty laws in regions like the EU are addressed by localized data centres and specific data handling protocols that comply with GDPR while still aligning with AWS's global security policies.

AWS also ensures that all employees, regardless of location, receive uniform security training that is updated regularly to address the latest security challenges and threat landscapes. This training is complemented by regular security assessments and audits which help to identify and rectify any deviations from the company's security standards across its operations.

15. Conclusion

This report has conducted an exhaustive evaluation of the security vulnerabilities within AWS's infrastructure. Utilizing established frameworks such as NIST and ISO/IEC 27001, we have identified critical areas of concern that could potentially compromise our operational integrity and customer trust. Notable vulnerabilities include misconfigured S3 buckets, inadequate IAM role management, and outdated software on EC2 instances. These vulnerabilities not only pose risks to data confidentiality and integrity but also threaten to disrupt the continuous service provision that is crucial for our client base.

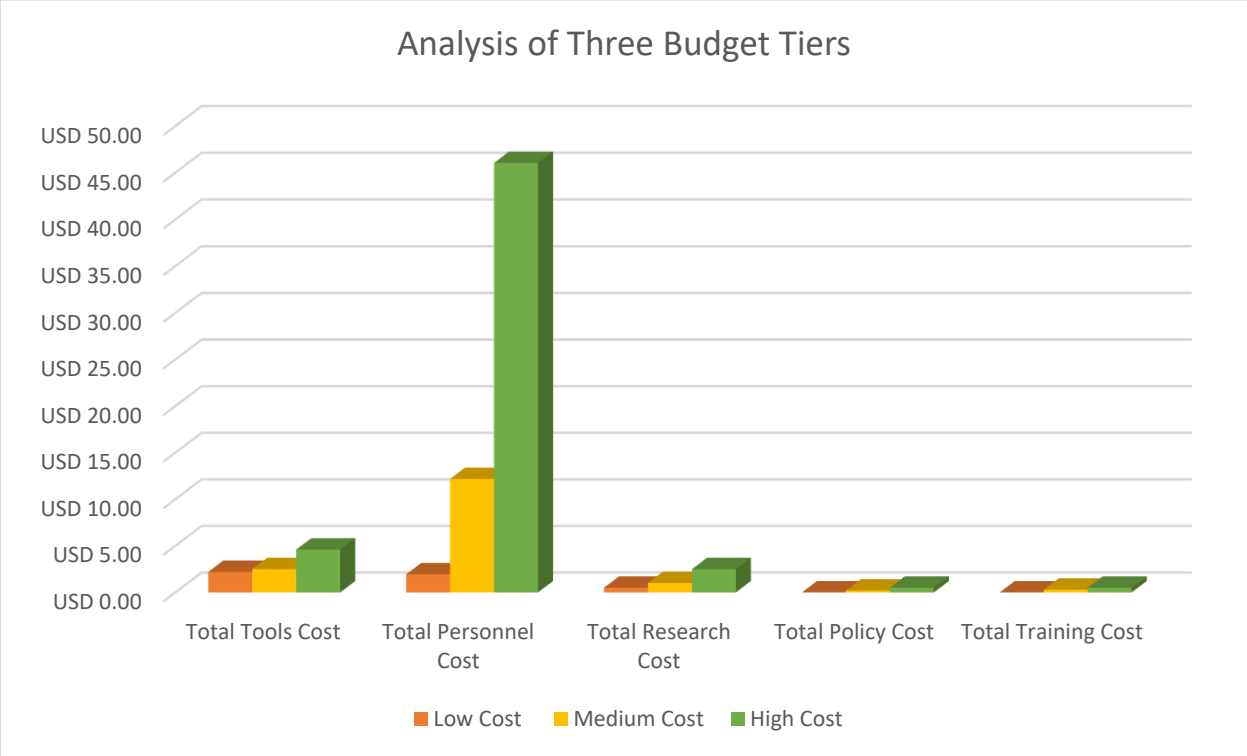

Fig. 1.12 - Cost of different control categories in Million $

In response to these findings, a tiered budgeting strategy was formulated to address these vulnerabilities in a manner that balances impact and cost-efficiency. The budget scenarios—low-cost, medium-cost, and high-cost—are designed to provide scalable solutions that meet varying levels of organizational need and risk tolerance. The security budget across different categories can be seen in Fig. 1.12. For instance, the high-cost budget allocates substantial resources towards comprehensive coverage across all potential threats, while the low-cost budget focuses on the most pressing risks with cost-effective solutions.

The cybersecurity landscape is dynamic, with new threats emerging continually. It is imperative that AWS not only implements the recommended measures but also commits to ongoing monitoring and reassessment of its security protocols. This includes staying updated with the latest cybersecurity research, evolving industry standards, and regulatory requirements. An agile, responsive approach to cybersecurity management will ensure that AWS remains ahead of potential threats and maintains its reputation as a secure and reliable cloud service provider.

Finally, the integration of these cybersecurity measures into AWS's broader operational and business strategies is crucial. By aligning our cybersecurity initiatives with business goals, AWS can ensure that its investments in security translate into enhanced service reliability, customer satisfaction, and business growth. This alignment supports AWS’s position as a leader in the cloud computing industry, not only in terms of market share but also in setting standards for security and reliability.

16. References

[i] https://www.nist.gov/document/aws-csf-20-response

[ii] https://aws.amazon.com/compliance/nist/

[iii] https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

[iv] https://aws.amazon.com/compliance/iso-27001-faqs/

[v] https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-3:v1:en

[vi] https://aws.amazon.com/compliance/iso-certified/

[vii] https://www.glassdoor.com/Overview/Working-at-Amazon-Web-Services-EI_IE7470741.11,30.htm

[viii] https://en.wikipedia.org/wiki/Amazon_(company)
[ix] https://www.britannica.com/topic/Amazoncom
[x] https://www.officetimeline.com/blog/amazon-history-timeline
[xi] https://fourweekmba.com/amazon-vs-walmart/

[xii] https://www.cnbc.com/2024/04/30/aws-q1-earnings-report-2024.html

[xiii] https://www.constellationr.com/blog-news/insights/aws-q4-revenue-growth-13-amazons-results-shine

[xv] https://aws.amazon.com/compliance/shared-responsibility-model/?ref=wellarchitected

[xvi] https://docs.aws.amazon.com/whitepapers/latest/public-sector-cloud-transformation/public-sector-cloud-transformation.pdf

[xvii] https://www.serveracademy.com/courses/introduction-to-aws-amazon-web-services/overview-of-aws-core-services/

[xviii] https://www.serveracademy.com/courses/introduction-to-aws-amazon-web-services/overview-of-aws-core-services/
[xix] https://aws.amazon.com/about-aws/global-infrastructure/
[xx] https://aws.amazon.com/systems-manager/features/
[xxi] https://docs.aws.amazon.com/whitepapers/latest/public-sector-cloud-transformation/public-sector-cloud-transformation.pdf

[xxii] https://betakit.com/another-round-of-layoffs-hits-amazon-employees-in-canada/