ΔΙΕΘΝΕΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Enhancing Security in Cloud Infrastructure: A Study and Framework Proposal for SMEs

Της φοιτήτριας.
Φάχμι Χριστίνα
Αρ. Μητρώου: 144325

Επιβλέπων
Ηλιούδης Χρήστος

Ημερομηνία Αύγουστος 2024

Τίτλος Δ.Ε: Enhancing Security in Cloud Infrastructure: A Study and Framework Proposal for SMEs
Κωδικός Δ.Ε: 23297
Ονοματεπώνυμο φοιτητή/τών: Φάχμι Χριστίνα
Ονοματεπώνυμο εισηγητή: Ηλιούδης Χρήστος
Ημερομηνία ανάληψης Δ.Ε: 30/10/2023
Ημερομηνία περάτωσης Δ.Ε: 27/08/204

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως διπλωματική εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

To my parents

Preface

This thesis was written and developed by Fachmi Christina under professor's Mr. Ilioudis Christos supervision. It focuses on studying cloud security threats and policies and developing an AWS framework for small-medium Greek organizations.

As security is a critical part of infrastructure development on cloud, goals were set to understand and determine key security threats in cloud environments, analyze existing security policies, and ultimately develop a tailored AWS security framework specifically for small-medium Greek organizations.

This framework development benefits organizations as it enhances their security posture, ensuring compliance, and providing adaptable policies that can evolve with emerging threats and technologies safeguarding AWS environments.

Περίληψη

Το cloud έχει εξελίξει τον τρόπο που χρησιμοποιούν οι εταιρείες την υπολογιστική υποδομή μέσω των χαρακτηριστικών του (π.χ., αυτοεξυπηρέτηση κατά απαίτηση, ευρεία δικτυακή πρόσβαση, συγκέντρωση πόρων κ.λπ.), καθιστώντας το επιθυμητό. Πάροχοι νέφους όπως AWS ή Microsoft Azure, φέρνουν αρκετά πλεονεκτήματα, όπως υψηλή διαθεσιμότητα, καθώς τα δεδομένα είναι προσβάσιμα από οπουδήποτε και οποτεδήποτε και επιτρέπουν τη μέγιστη παραγωγικότητα και αποτελεσματικότητα των επιχειρήσεων, διασφαλίζοντας ότι οι εφαρμογές είναι πάντα προσβάσιμες. Επιπλέον, η υλοποίηση είναι απλή, καθώς οι επιχειρήσεις μπορούν να διατηρήσουν τις ίδιες εφαρμογές και επιχειρηματικές διαδικασίες χωρίς να αναλώνουν χρόνο ή πόρους για τεχνικά ζητήματα. Επιπρόσθετα, παρέχουν ευελιξία και είναι αποτελεσματικές στην ανάκτηση δεδομένων.

Παρά τα πλεονεκτήματα αυτά που προσφέρει το cloud, είναι αναγκαίο να ληφθεί υπόψη ο παράγοντας της ασφάλειας καθώς εμφανίζονται νέες προκλήσεις στην ισορροπία μεταξύ παραγωγικότητας και ασφάλειας. Συνήθως, οι πάροχοι cloud ακολουθούν τα πρότυπα ασφαλείας της βιομηχανίας προστατεύοντας την ακεραιότητα των διακομιστών τους. Ωστόσο, οι οργανισμοί οφείλουν να εξετάζουν τους τρόπους όπου μπορούν να προστατεύουν τα δεδομένα και τις εφαρμογές που φιλοξενούνται στο cloud. Για παράδειγμα, δεν είναι σπάνιο να χάνεται ο έλεγχος όσον αφορά ποιοι άνθρωποι ή ακόμη και εφαρμογές έχουν πρόσβαση σε ποιο είδος πληροφορίας. Επιπλέον, σε πολλές περιπτώσεις, οι υποδομές των πελατών φιλοξενούνται υπό την ίδια υποδομή, με αποτέλεσμα να εγκυμονείται ο κίνδυνος οι υπηρεσίες να εκτεθούν, οδηγώντας τες σε παρεμπίπτουσες ζημίες. Τέλος, λανθασμένες ρυθμίσεις, όπως η αδυναμία δημιουργίας ισχυρών κωδικών ή η έλλειψη εφαρμογής κατάλληλων πολιτικών και ρυθμίσεων ασφαλείας, παραμένουν ένα από τα μεγαλύτερα προβλήματα που αντιμετωπίζουν οι εταιρείες κατά τη μετάβαση από τη φυσική υποδομή στο cloud, καθώς οδηγούν σε εσωτερικές απειλές.

Ο στόχος αυτής της διπλωματικής είναι η σφαιρική μελέτη των υλοποιήσεων ασφάλειας στις υποδομές νέφους. Αρχικά, θα τεκμηριωθούν γνωστοί κίνδυνοι, επιθέσεις καθώς και θα συζητηθούν τρόποι αντιμετώπισης. Στη συνέχεια, θα γίνει μια λεπτομερής ανάλυση των πλαισίων ασφαλείας του cloud για την προστασία των πόρων σε παρόχους όπως η AWS και η Microsoft Azure. Τέλος, θα παρατεθεί ένα πλαίσιο ασφάλειας στο cloud όπου θα αποσκοπεί στην ανθεκτικότητα μικρών και μεσαίων επιχειρήσεων.

« Enhancing Security in Cloud Infrastructure: A Study and Framework Proposal for SMEs »

«Christina Fachmi»

Abstract

As the cloud has revolutionized business, more organizations choose to implement their infrastructure and host their services on the cloud. Cloud providers like AWS or Microsoft Azure, bring several advantages like high availability as data is accessible from anywhere and at any time. The enterprise productivity and efficiency are minimized by ensuring applications are always accessible. Moreover, the implementation is easy as businesses can keep the same applications and business processes without having to deal with the backend technicalities. On top of these, they also provide flexibility as cloud services are scalable and efficient recovery.

Besides these advantages cloud computing can offer, when choosing the cloud approach, businesses need to take into consideration the security factor as new challenges arise when balancing productivity levels and security. Typically, most cloud providers adhere to industry-standard security practices and proactively protect the integrity of their servers. Nevertheless, organizations still need to assess how to protect data and applications hosted on the cloud. For instance, in the realm of cloud computing, it's not unusual to lose sight of which individuals or even applications can access what kind of information. Also, in several cases, customer infrastructures are hosted under the same umbrella, and this inevitably entails the risk of services being compromised leading to collateral damage. Finally, misconfigured assets like not creating strong administrative passwords or the lack of implementation of proper security policies and settings are still one of the biggest issues that companies are facing when migrating their physical infrastructure on the cloud as they lead to unintended inside threat.

This thesis' goal is the comprehensive study of security implementations on cloud infrastructures. First, known risks and attacks will be documented as fixes and implementations. Then, a thorough analysis of existing cloud security frameworks for protecting cloud resources in cloud providers like AWS and Microsoft Azure will be provided. Finally, a cloud security framework will be provided that will aim at small to medium businesses resilience.

Acknowledgements

Firstly, I would like to thank my family for their support from the beginning of my studies, till the completion of this thesis. Their understanding, support, courage, motivation and patience were the most important elements for the successful completion of this thesis.

I would also like to thank my professor Mr Christos Ilioudis for his assistance and guidance regarding my thesis goals.

Finally, I would like to thank my friends for their support and encouragement that really helped me to complete this assessment.

Table of Contents

List of Figures

List of Tables

Glossary

SME	Small-Medium Enterprise
AWS	Amazon Web Services
DoS	Denial of Service
MitM	Man-in-the-Middle Attacks
IRP	Incident Response Plan
BCP	Business Continuity Planning
SIEM	Security Information and Event Management
SEM	Security Event Management
SIM	Security Information Management
EDR	Endpoint Detection and Response
ZT	Zero Trust

MFA	Multi-factor Authentication
CIS	Center for Internet Security
CSA STAR	Cloud Security Alliance's Security Trust Assurance and Risk
ISO	International Organization for Standardization
CCM	Cloud Controls Metrics
CAIQ	Consensus Assessments Initiative Questionnaire
GDPR	General Data Protection Regulation
IEC	International Electrotechnical Commission
PII	Personally Identifiable Information
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
DSDM	Dynamic Systems Development Method
MoSCoW	Must Have, Should Have, Could Have, Won't Have this time
CISO	Chief Information Security officer
IAM	Identity and Access Management
AMI	Amazon Machine Image
KMS	Key Management Service
DAX	DynamoDb Accelerator
EBS	Elastic Block Service
EC2	Elastic Compute Cloud
EFS	Elastic File System
RDS	Relational Database Service
S3	Simple Storage Service
DLP	Data Loss Prevention
SSL	Secure Sockets Layer
ACL	Access Control Lisτ
SQS	Simple Queue Service
EDR	Elastic Disaster Recovery

RTO	Recovery Time Objectives
RPO	Recovery Point Objectives
DNS	Domain Name System
VPC	Virtual Private Cloud
SSH	Secure Shell
RDP	Remote Desktop Protocol
API	Application Programming Interface
CMK	Customer Master Keυ
NACL	Network Access Control List
SNS	Simple Notification Service
VPN	Virtual Private Network
GCP	Google Cloud Platform

Chapter 1: Introduction

1.1 Thesi's Goals

This thesis' goal is the comprehensive study of cloud security threats and security implementations on cloud infrastructures.

1.2 Accomplishments

This framework development benefits organizations by strengthening their security measures, maintaining compliance, and implementing flexible policies that can adapt to new threats and technologies, ensuring the protection of AWS environments.

1.3 Thesis Structure

First known risks and attacks will be documented. Then, a thorough analysis of existing cloud security frameworks for protecting cloud resources in the cloud will be provided. Afterwards, a cloud security framework will be provided that will aim at small to medium businesses that their infrastructure exists in AWS.

Chapter 2: Security Challenges and Threats

2.1 Introduction to Cloud Infrastructure

Cloud computing has gradually merged into organizations' operations, contributing to their efficiency by providing high availability, scalability, and cost reduction. Cloud computing's goal is to offer innovation and flexibility. [1,2]

Companies, including Amazon Web Services(AWS), Google, IBM, Microsoft, are successfully developing cloud-based products and technologies. For instance, AWS top product categories include computing, storage, databases, networking, machine learning, security, etc. [3]

Cloud computing has rapidly become a popular solution for delivering computing services. It has transformed IT infrastructure usage, as its primary goal is to offer flexibility, instant access to computing resources, network availability, and the capability to share resources efficiently. These attributes have made cloud computing the most preferred choice for various applications. However, security should always be a priority. Cloud computing offers several advantages, but risks and threats related to cloud security exist and continue to evolve. [4]

2.2 Cloud Security

Cloud security is a crucial aspect of IT infrastructure, encircling a range of tools to protect systems, data, and applications from risks. As industries gradually embrace cloud computing for its advantages like adaptability, high availability, and cost efficiency, they also face unique challenges. These challenges include:

- Data privacy protection.
- Always keep compliance with regulatory standards.
- Protect against and respond to evolving cyber threats.

Effective cloud security requires an approach, in which various security mechanisms such as administrative controls, physical security measures, technical safeguards, and operational practices can be integrated. Following this kind of strategy verifies that both the cloud infrastructure and the sensitive information and data in general are protected against unauthorized access, data breaches, and other cyber risks. Using cloud services requires integrity, confidentiality, and continuous availability. [5, 6]

2.3 Data Leakage and Privacy

The storage and transmission of data in cloud environments is often managed by third-party providers, and this raises concerns about data loss, and unauthorized access [1].

Data loss in cloud computing is a significant challenge that can have extensive consequences for organizations. Hardware failures and software glitches or human errors, such as accidental deletion or corruption of data system failures, cyber-attacks, or even provider outages can lead to permanent data loss. Indeed, a great percentage of businesses identify this as their most significant concern regarding cloud security. When any kind of data like a cloud-based repository are shared online with no proper access settings enabled, they become accessible to anyone who may get the URL path.

Moreover, cloud services usually involve dependencies on third-party providers. These providers may encounter security issues like system outages or services disruptions, which can inadvertently lead to data loss for their clients. Additionally, the continuous evolution of cyber threats poses a continual important risk. Attacks such as ransomware or targeted breaches can result in significant data loss, either through direct deletion or through encryption by malicious actors. [7]

2.4 Identity and Access Management

Identity and Access Management (IAM) is a fundamental part of cyber security. It guarantees that the appropriate individuals have the proper access to data, services, applications and resources in general. In cloud infrastructures, IAM systems come across critical risks and threats that increase the risk of data breaches and leaks.

- *Credential Compromise*
  Credential compromise occurs when attackers steal usernames, passwords or security questions to access resources like accounts, systems, services and applications. Credentials can be exposed through various methods.
  One very common attack is when attackers use social engineering techniques or compose emails and create websites that are almost identical to original services to make users reveal their credentials. Once credentials are obtained, attackers can access sensitive cloud resources, sensitive data, and usually escalate privileges. As time passes by, these schemes come closer to original ones(same text, pictures, legitimate contact information) making it hard for users to identify fake emails and websites from the legitimate ones.

  Moreover, attackers use tools to guess passwords continuously through trial and error (brute force) or exploit lists of compromised credentials from previous breaches (credential stuffing). In the cloud, systems can be exposed as users tend to use one password, or weak passwords (birthdays, names, phone numbers, etc) for all their accounts and unauthorized access can lead to data theft or loss, unauthorized transactions, and further exploitation of cloud resources. So strong password policies are crucial to prevent credential compromises.

- *Insider Threats*
  Insider threats are related to employees or other trusted users that accidentally expose their credentials or share sensitive documents without following security procedures leading to data leakage. Users with harmful intentions can steal data or sabotage systems, leveraging their original access, which makes detection difficult and consequences include but not limited to financial loss, reputational damage, and regulatory penalties.

- *Poorly Managed Privileged Accounts*
  Accounts with privileged access, such as those belonging to system administrators or team leaders, provide broad access to cloud resources and security policies are crucial. Granting excessive privileged access heightens risk, as users with broad access might unintentionally or deliberately take actions that jeopardize security, such as modifying configurations or setting up unauthorized access points.

- *Lack of Monitoring and Logging*
  A lack of monitoring and logging system can result in undetected misuse by privileged users, compromised accounts, or delay incident response potentially leading to data theft, service

disruptions or even legal penalties.

- *Week Authentication Methods*
  Using weak authentication methods such as a disabled multi-factor authentication future or static credentials that are not regularly rotated, and not strong enough can be easily stolen and reused by attackers, granting persistent access to resources and enabling long-term data exfiltration and system manipulation.

- *Third-Party Access Risks and API Vulnerabilities*
  Providing third-party vendors and partners with access to cloud resources can introduce significant security risks, as these external entities may not meet the same security standards, potentially creating gaps and elevating security risks. This issue is exacerbated by vulnerabilities in APIs used for IAM in cloud environments, which can be prone to various types of attacks. [8,9]

2.5 Epilogue

The dynamic nature of cloud computing introduces both opportunities and risks. To navigate this complex landscape, organizations must remain committed to always update their security practices, embrace advanced technologies, and foster a culture of security awareness. By prioritizing data protection, creating and implementing Identity and Privileged Access Management policies, companies can better protect their assets, maintain compliance, and preserve the trust of their customers and stakeholders in an increasingly interconnected world.

Chapter 2

Chapter 3: Common Cyber and Cloud Attacks

3.1 Introduction

As cloud usage keeps increasing, important cybersecurity challenges impact organizations. Common attacks, such as phishing, social engineering, password attacks, malware, and denial-of-service (DoS) attacks, take advantage of misconfigurations in systems and in security policies, like weak passwords, to gain unauthorized privileged access to sensitive data or disrupt crucial operations. Moreover, threats now include attacks that are specifically targeting cloud infrastructures causing data leaks, exposed user or application accounts, and interfaces lacking security. These attacks take advantage of the distributed nature of cloud systems putting them in jeopardy and highlight the importance of strong security measures to keep data secure.

3.2 Common Attacks

Cyber-attacks appear in various ways, each exploiting different vulnerabilities. Below there is an overview of some of the most common types of cyber-attacks.

3.2.1 Phishing

Attackers send emails or messages that are almost identical to original sources, such as banks or well-known companies. These messages include links to redirect the recipients to fake websites that look almost the same as the legitimate ones. The difference usually relies on a part of the URL link or syntax/grammar errors, and they prompt users to act quickly in an urgent situation. These attacks aim for people to provide credentials and share sensitive information, mostly credit card numbers. According to Gary Smith, in his article on StationX, during 2023, 58% of businesses with cloud environments reported a phishing incident. The figure below illustrates phishing statistics per category. [12]

Image 3.1: Phishing Statistics [12]

3.2.2 Malware

Malicious software (Malware) is a kind of attack where software is created with the only purpose to harm, damage, or disable computers, servers and networks. Common types of malwares include bots, viruses, worms, trojans horses, keyloggers and spyware. Malware usually spreads through email attachments (document files, photos, etc.), websites that are hijacked, or software that a user can download and run on their computer. Their goal is to steal sensitive information, monitor and track user activity, or even take control of infrastructures.

3.2.3 Ransomware

Ransomware is a type of malicious software. Ransomware is used to encrypt a victim's content and lock them. The attacker demands a bribe payment to free the data. Ransomware is spread through phishing emails as they are hidden in attachments and if a user opens this attachment, it affects their computer.

3.2.4 Denial-of-Service (DoS) Attacks

Denial-of-Service (DoS) attack is caused by a source that floods a system, network, or website with so many requests that they fail to respond to legitimate users' requests. Distributed Denial-of-Service (DDoS) attacks are similar, but they consist of several sources all working together to flood the target with traffic. These attacks can cause slowness, disrupt services or even shut down a server. [10]

3.2.5 Man-in-the-Middle (MitM) Attacks

Man-in-the-Middle (MitM) attacks occur when an attacker inserts in a communication between two parties without their knowledge and for that reason is called "man-in-the-middle" attack. With this type of attack, not only sensitive data can be stolen, but attackers may produce text messages (with bot usage) impersonating a legitimate person in order to extract information and access other system devices. This can happen through various methods, such as email hijacking, DNS spoofing, stealing browser cookies or unsecured Wi-Fi networks, allowing attackers to steal sensitive data or inject malicious content. [13]

3.2.6 SQL Injection

In SQL injection attacks, attackers insert malicious SQL code queries into input fields usually in websites. A successful SQL injection leads applications into executing commands that can read, or even modify databases. This not only can lead to unauthorized access to crucial information but can also cause data loss. [14]

3.3 Cloud Attacks

Cloud computing is a double-edged sword as it provides great advantages to organizations, but at the same time presents opportunities for attackers to exploit weaknesses. Some of the most frequent cloud attacks are listed below.

3.3.1 Data Breaches

Weak security policies, or weak and expired passwords, can help an attacker to gain access to unauthorized accounts or services, and as a result, they gain access to sensitive and crucial information, causing data breaches. Data breaches lead to data loss or even legal violations. According to an IBM data breach report, there is a 10% increase in average cost of data breaches that corresponds to almost 5 million USD [15].

3.3.2 Security Misconfigurations

Cloud computing services configuration is crucial for protection against threats. Security misconfigurations can include misconfigured access controls, weak passwords that are not updated regularly, lack of multi-factor authentication or systems that are not updated in an acceptable time manner. [16,17]

3.3.3 Cloud Storage Misconfiguration

Cloud storage configuration misconfiguration can lead to data leaks or data loss. For instance, a cloud storage that instead of private has public access or storage with encryption disabled, are easy targets for attackers. Moreover, when versioning control is missing, data that is lost cannot be recovered. [16,17]

3.3.4 User Account Compromise

A user account is compromised when an attacker gains access to it through the same user owner. Most common cases are the ones that trick users to input their credentials. It is important to highlight here that this differs from account hijacking where an attacker gains access that is not authorized to an account through methods like social engineering or taking advantage of weak passwords and the lack of multi-factor authentication. In both cases, once an attacker gains access, they can view or edit confidential information, modify or delete data. [17]

3.3.5 Cloud Malware Injection Attacks

There are attacks where malicious software is being injected into cloud services. As a result, the attacker can either use them as their own or they can steal, modify and delete data. This can be accomplished in several ways some of them are:

- Taking advantage of cloud services and applications weaknesses.
- Obtaining unauthorized access to accounts and injecting malware through document files or links. [17]

3.3.6 Insider Threats

Insider threat is a form of threat where employees inside an organization that already have access to cloud services, misuse this access or accidentally put in jeopardy sensitive information. [17]

3.3.7 Insecure APIs

APIs and interfaces are often provided for users to interact with while using cloud services. However, interfaces that lack proper security configurations and APIs with vulnerabilities can be easy targets for attackers to access and modify or delete data. [17]

3.3.8 Real World Cloud Attacks Examples

According to Amit Seps article in Aqua cloud native wiki, several organizations, even huge ones, come across cyber security attacks. He lists several example and some of them are:

Facebook
In April 2021, Facebook identified a vulnerability that millions of user records were affected by. Facebook said the problem was an exposure on Amazon Web Services AWS servers related to databases that contained sensitive information that could be used for social engineering and phishing attacks and was identified and fixed directly. [17]

Verizon
In 2017, a huge telecommunications organization, Verizon Communications, experienced a series of cloud-related security incidents. Verizon's partner, Nice Systems, due to a fault in its Amazon S3 bucket that was used as configuration storage, accidentally exposed user information. Then in 2020, Verizon experienced 29,207 security incidents, of which 5,200 were confirmed compromises. The attacks included DDoS, social engineering, and client-side web application flaws that led to compromise of server-side systems. Verizon said most of these attacks were due to the "human element", because of remote work during the COVID-19 crisis. [17]

3.4 Epilogue

As cloud technology continues to thrive, it is important for organizations and individuals to be aware of cloud threats like the ones we discussed in this chapter. Continuous updates, awareness, and employees' training to recognize phishing emails that as time passes become more identical to legitimate messages or websites or even to create strong account passwords to prevent attackers from account hijacking and by extension data leaks, can make an impact in threats detection and successful mitigation.

Chapter 3

Chapter 4: Recovery Strategies

4.1 Introduction

In the cybersecurity sphere, the continuous and rapid evolution of cyber-attacks highlights the importance of creating recovery plans, procedures to ensure that the services a business provides continue uninterrupted and limit damages. These procedures can provide the necessary instructions for preparation and response to cyber-attacks. This chapter focuses and dives into useful and efficient recovery methods that are able to prepare and support enterprises in the event of a security attack.

4.2 Supporting Mechanisms

4.2.1 Incident Response Plan

An Incident Response Plan (IRP) is the foundation for efficient recovery procedure. It outlines the mandatory steps to go through in case of a security incident. It contains responsibilities per role and communication protocols in full detail. It is crucial for enterprises to create, test and keep updated IRPs as they can contribute to direct identification and response to attacks, especially to new kinds of threats, while minimizing damage or service disruptions. An IRP contains some key elements like threat identification, escalation procedures, quick response actions and reporting techniques. According to Mohanakrishnan's article the incident response lifecycle and incident response best practices are represented in images 4.1, 4.2 respectively. [18]

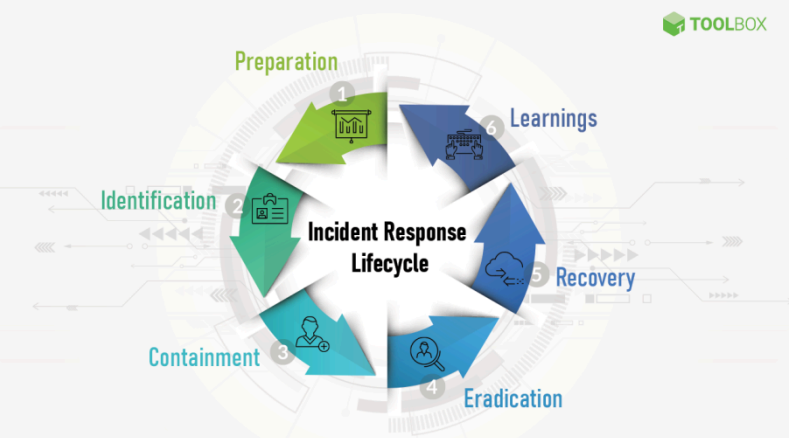

Image 4.1: Incident response lifecycle [18]

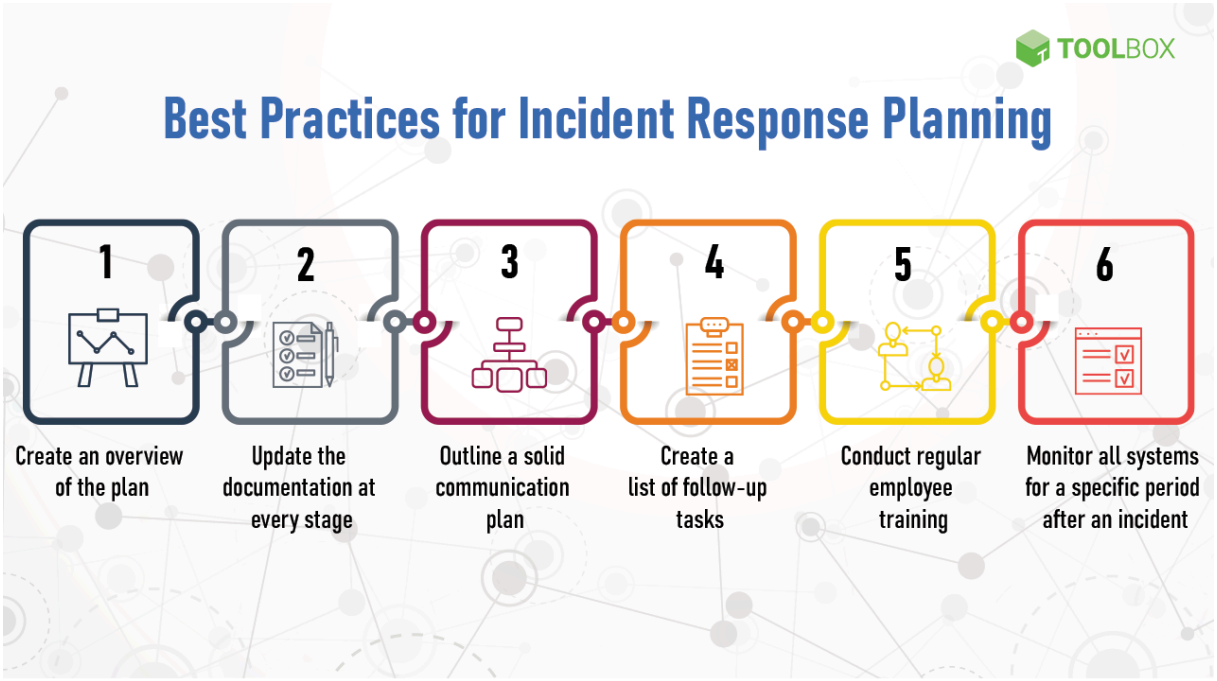

Image 4.2: Incident response planning [18]

4.2.2 Data Backup and Recovery

Regular and consistent data backups are a very important strategy for a successful recovery as businesses rely on them for not only recovering data after a security incident like unauthorized access or malware but for damage control. Backup procedures should be stored ideally to external devices or(and) to cloud storages to guarantee protection from physical damage. Finally, backups should be checked regularly to ensure that data are not corrupted and restore process runs smoothly.[19]

4.2.3 Business Continuity Plan

Business Continuity Planning (BCP) , is a key part of every recovery strategy because not only business can rely on it when it comes for recovery, but also includes procedures to address the complete durability of an enterprise. BCP embodies strategies in order to maintain crucial business operations throughout a crisis. It consists of communication methods, system management, and mostly employee safety. An extensive BCP guarantees that all elements of the organization remain functional, even when encountered with significant disruptions. Exercises and updates that take place constantly to the BCP help organizations to be prepared for various cases and ensure that recovery actions are coordinated and effective.[20]

4.2.5 Threat Intelligence

Threat intelligence encompasses several elements like gathering data, analyzing, and utilizing them for prospective and present threats to instruct strategies to use as defense. For organizations to be able to better prepare and act in an attack event, they are required to recognize and understand the methods, procedures used by attackers. This is vital for organizations as real-time alerts can be created in case of an emergency and they can tailor their security policies in advance. [21]

4.2.6 Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) systems stem from the combination of two different components, Security Event Management (SEM) and Security Information Management (SIM). Security Event Management (SEM) systems can monitor systems in real time using agents and controlling the events that occur in them. The SEM agent can segregate information and as a result can send to a SEM manager only the legitimate events as logs. The Security Information Management (SIM) systems can collect and retain data in central data storage for a period not exceeding 2 years. As a result, other mechanisms can access and analyze the data. [22] By collecting, storing and evaluating data, SIEM systems are capable of identifying threats in an early stage providing organizations the ability to respond immediately and strengthen recovery attempts. The SIEM architecture and process flow are illustrated in images 4.3 and 4.4 in Remya Mohanan article in Spiceworks. [23]

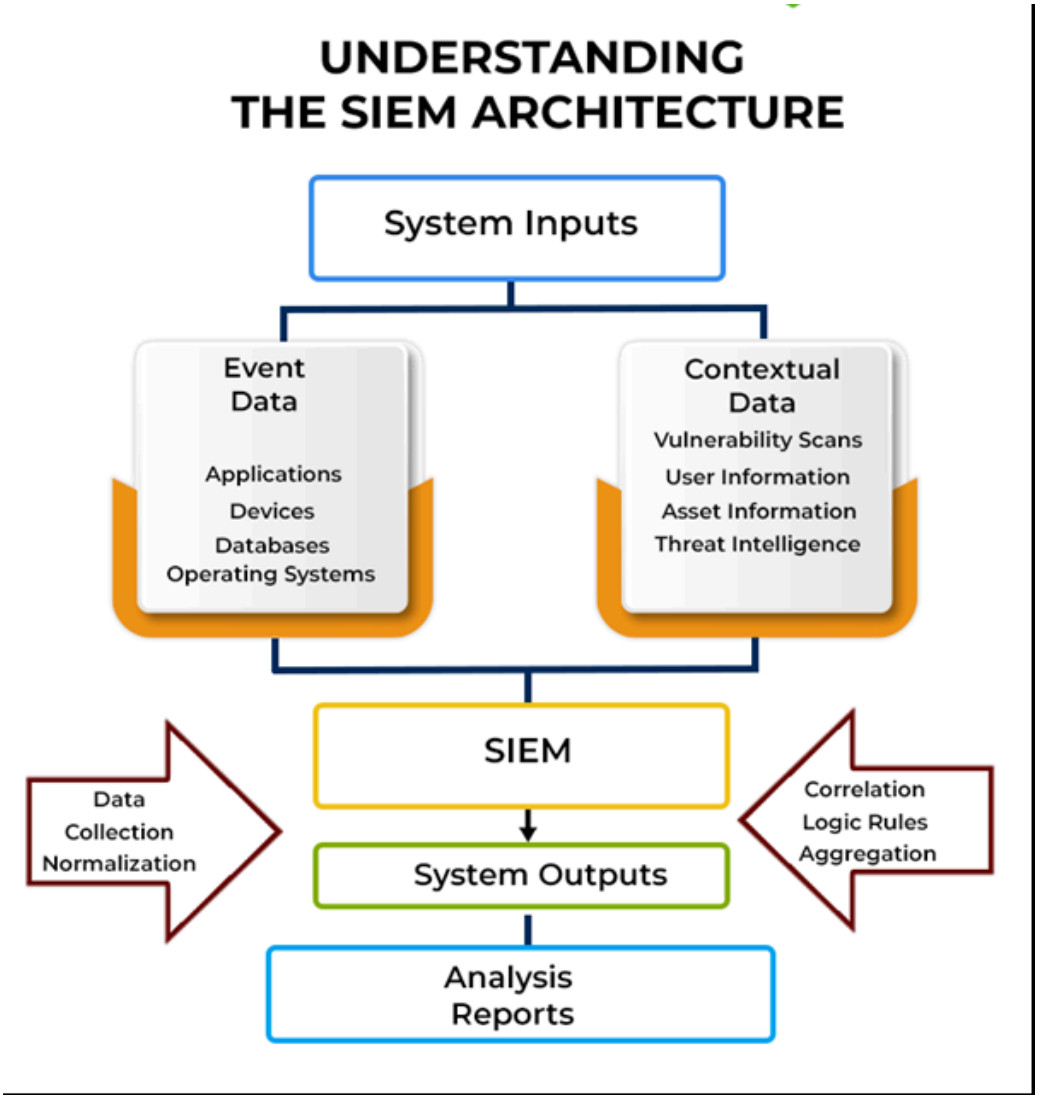

Image 4.3 SIEM Architecture [23]

Image 4.4 SIEM Process Flow [23]

4.2.7 Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR) solutions have as a primary goal to monitor and respond to singular endpoints' actions, such as computers and mobile devices. These tools' advantage is that they can bring full visibility into endpoint performance and activities, find actions that are unusual, and respond fast to potential threats. EDR solutions play a significant role as they can detect threats before they spread. Image 4.5 by Openedr, provides more details on EDR's primary functions. [24, 25]

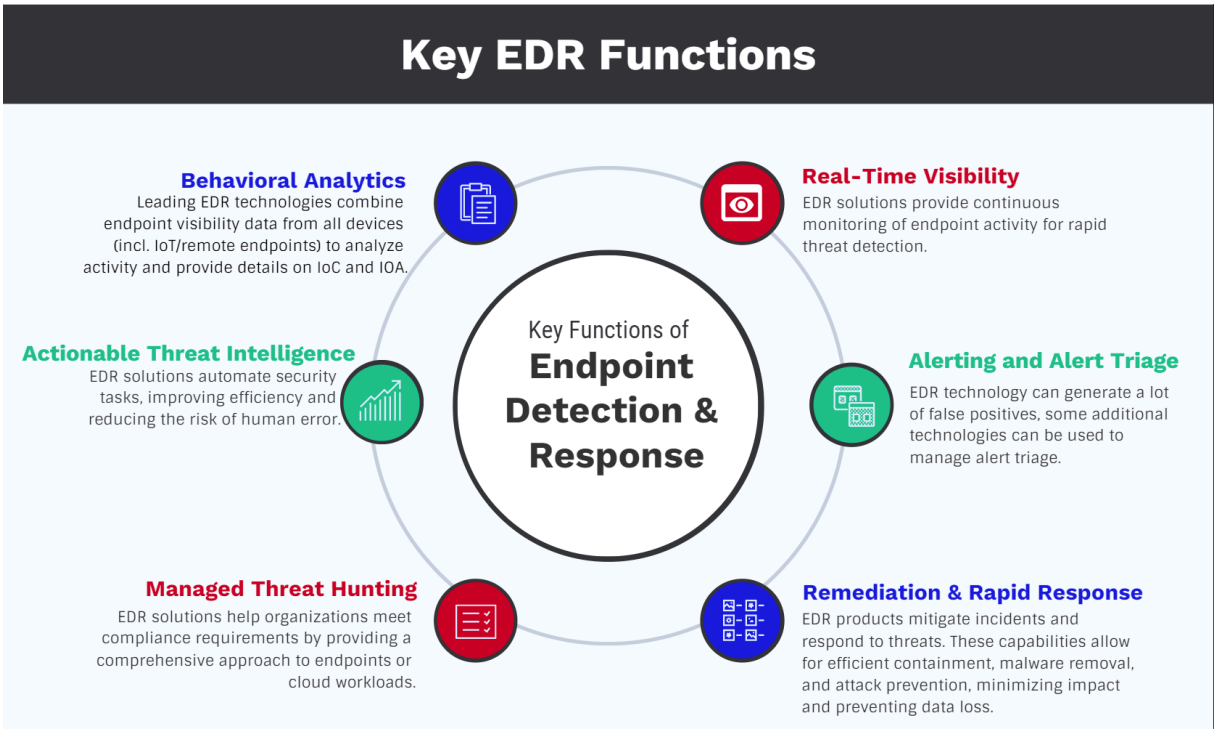

Image 4.5: Key EDR Functions [25]

4.2.8 Employee Training and Awareness

Training and awareness programs that occur frequently can contribute and be effective in cyber-attacks reduction. Employees should have knowledge about security best practices and be aware of potential threats like phishing, create strong passwords, and follow security protocols.

4.3 Epilogue

Recovery procedures are key components of a comprehensive cybersecurity framework. As discussed, successful recovery from cyber and cloud attacks relies on incident response plans and strategies that are well organized, strong data backup systems, extensive disaster recovery and business continuity plans and strategies. Moreover, organizations should regularly check, test and keep their recovery mechanisms updated to always be prepared and safeguard their assets.

Chapter 4

Chapter 5: Cloud Security Frameworks

5.1 Introduction

This chapter contains an overview of cloud security frameworks, and security best practices that organizations can utilize to safeguard their cloud infrastructure.

5.2 Evaluation Principles

The shift to cloud services is bringing security challenges among the advantages. In order to secure cloud environments, fundamental security principles should be established. Organizations cloud security strategies should be aligned with these principles by maintaining a risk-oriented manner, deploying strategies and tactics for efficient defense, and provide monitoring tools and improvements.[26]
Some of key guidelines include:

5.2.1 Zero Trust

Zero Trust (ZT) is a security model that its principle relies on the fact that no one can be trusted. The ZT principle includes identity verification that is requested for all individuals and electronic devices to gain access to resources located on a private network. Zero Trust principles include:

- *Monitoring and validation*
  As neither individuals or devices from inside or outside of the network can be trusted and attackers may exist even within the organization's network, Zero Trust prompts both users and devices to regularly verify their identity and privileges with logins and connection timeouts.

- *Least Privilege Access*
  Users in an organization have different roles depending on their position, team, or even a project they work on. According to the Zero Trust principle, users should only gain access to what they really need to access.

- *Device's Monitoring*
  Alongside users' access, ZT systems should be able to monitor devices that access the network to verify that all devices are authorized access, and they are not compromised.

- *Lateral Movement*
  Lateral movement is when an unauthorized user (attacker) gains access inside the network and moves within the network. After initial access, attackers expand their access through the services and data making it challenging to identify lateral movement even if the entry point has been detected. The Zero Trust principle prevents attackers from lateral movement as it periodically forces users for authentication and compromised devices, or user accounts can be detected in an early stage.

- *Multi-factor authentication (MFA)*
  Multi-factor authentication (MFA) is a significant part of Zero Trust security. MFA requires users to authenticate in more than one way. For instance, users can be authenticated with the combination of password and a code they get via email or a text message. Another example is the usage of applications that generate codes per application every few seconds so that users can authenticate themselves using their password and the code from the generator. [27]

5.2.2 Risk Assessment and Management

Regularly perform evaluations for security risks to detect vulnerabilities regarding the cloud environment and create a plan for mitigation actions. [26]

5.2.3 Compliance and Legal Requirements

Cloud providers should comply with security standards and regulations (e.g., GDPR, ISO/IEC 27001). Moreover, cloud services should meet the organization's legal obligations. [26]

5.2.4 Data Protection and Privacy

Data encryption is a fundamental part of data protection. Encryption should be applied both at rest and in transit as best practice in order to protect data from unauthorized access. Strength and implementation of encryption protocols need to be evaluated to meet industry standards and best practices. [26]

5.2.5 Resilience and Incident Response

Disaster recovery and business continuity plans should be checked regularly to ensure that mechanisms for quick recovery are responding with no issues. Also, incident response capabilities, focusing on the speed and effectiveness of their breach management, and verify that there’s a clear plan for coordination with your organization during incidents. [26]

5.3 Cloud Security Frameworks

Frameworks in cloud computing are sets of guidelines, controls and best practices that are used to help organizations to secure their infrastructure and to identify risks and protect against threats in cloud environments.

Some of the security frameworks consist of Center for Internet Security (CIS), Cloud Security Alliance's Security Trust Assurance and Risk (CSA STAR), ISO 27017 and ISO 27002:2022 [28]

5.3.1 Center for Internet Security (CIS)

The Center for Internet Security (CIS) is a nonprofit organization founded in 2000. CIS is well-known for the development of the CIS Controls and CIS Benchmarks frameworks for organizations. CIS aims to provide organizations with tools to configure secure cloud infrastructure and be protected from cyber attacks.

The CIS Critical Security Controls (CIS Controls) consist of a collection of custom best practices that businesses can use to protect against threats. CIS Controls include,

- Simplify Approach to Threat Protection
- Comply with Industry Regulations
- Achieve Essential Cyber Hygiene
- Translate Information into Action
- Abide by the Law
- CIS Benchmarks

The image below illustrates the basic, foundational and organizational controls according to CIS Critical Security Controls Version 7 – What's Old, What's New blog.

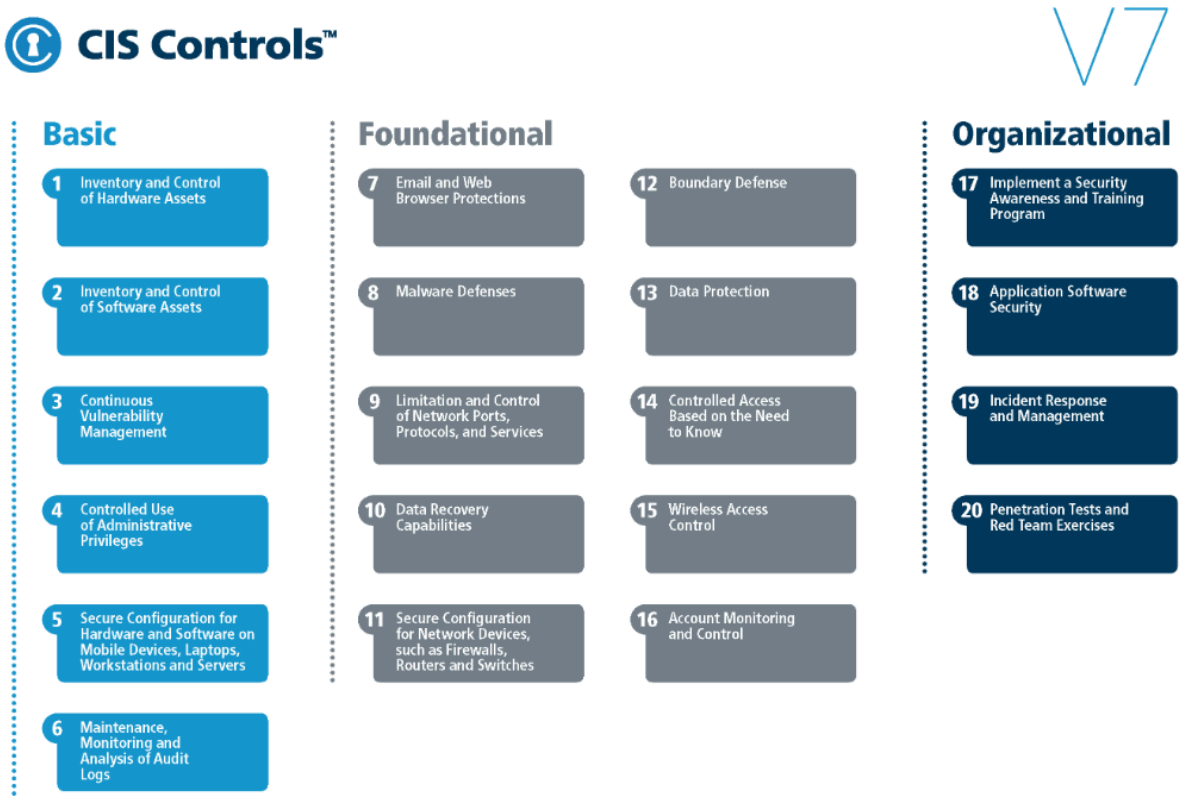

Image 5.1: CIS Controls [31]

The CIS Benchmarks are custom configuration instructions for more than 25+ vendor product categories including cloud providers, software, network devices, mobile devices, operating systems, and server software. They are developed by experts located all over the world and their goal is to help businesses to protect their infrastructures against risks. [29, 30, 31]

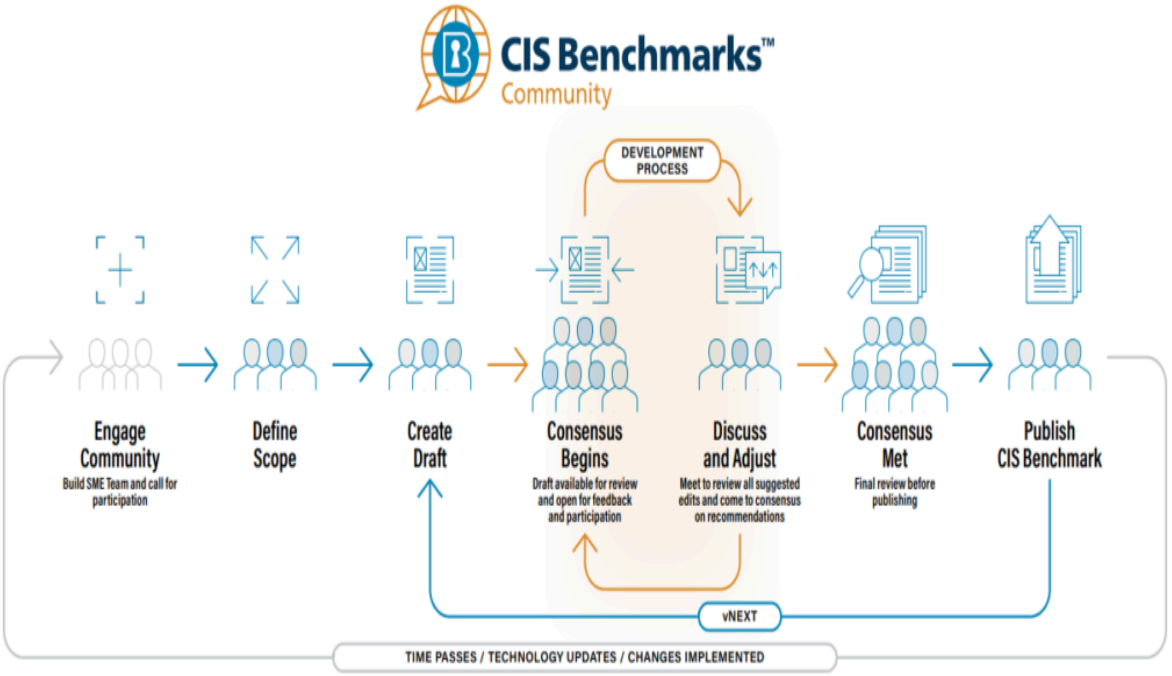

Image 5.2: CIS Benchmarks [32]

5.3.2 Cloud Security Alliance's Security Trust Assurance and Risk (CSA STAR)

The CSA STAR is an globally accessed registry that contains a list of the security and privacy procedures used by major cloud computing services. It embodies transparency, thorough auditing, and aligning standards principles, as defined in the Cloud Controls Matrix (CCM). By publishing their information to the STAR registry, organizations can demonstrate to existing and to potential clients their security strategies and compliance with various regulations, standards, and frameworks. This helps simplify the process by reducing the need to complete numerous customer questionnaires.[33]

5.3.2.1 The Cloud Controls Matrix (CCM)

The CSA Cloud Controls Matrix (CCM) is a framework that contains best practices for cloud computing security. It consists of 197 controls grouped in 17 domains. CCM can be used as a guide for implementing security policies within the cloud. The CCM now includes the following:

- CCM v4 Controls
- Mappings
- CAIQ v4
- Implementation Guidelines
- Auditing Guidelines
- CCM Metrics
- CCM Machine Readable (JSON/YAML/OSCAL) [34]

5.3.2.2 Structure of CSA STAR

According to CSA, there are two main levels for companies that submit to the STAR registry. Each level has its own requirements.

Level 1 is about Self-Assessment. There are 2 assessments. The security and the privacy self-assessment. Organizations can choose to either submit one or submit both assessments. Regarding the security assessment, organizations can choose to utilize the Consensus Assessments Initiative Questionnaire (CAIQ) which is aligned with the Cloud Controls Matrix to assess and record their security controls. Regarding the privacy assessment submissions, organizations can follow the guidelines outlined in the General Data Protection Regulation (GDPR) Code of Conduct Level 2. Level 1 includes the following variations:

- Security Self-Assessment
  The CSA STAR Self-Assessment is a service that records the security measures of different cloud service providers, allowing users to evaluate the security of the cloud providers they currently use or are considering using. Cloud providers complete the CAIQ to illustrate their compliance with the CCM. This data is made publicly accessible, enhancing transparency in the industry and giving customers insight into the security practices of each of the providers. STAR Self-Assessments are reviewed and updated every year.
- The CAIQ v4 is available in two editions:
  - CCM + CAIQ v4: The CAIQ v4 in combination with CCM. The CCM can serve as a point of reference. When it comes to submission, organizations should only submit the CAIQ file.
  - Security Questionnaire (CAIQ v4): File for filling and submission to the STAR registry.
- GDPR Self-Assessment
  The GDPR Code Self-Assessment is all about how well a cloud service provider's offerings adhere to GDPR regulations. When an organization completes the submission procedure, receives a Compliance Mark which is a badge that proves an organization meets the requirements by GDPR. This badge is valid for 1 year.

The Self-Assessment should be updated whenever there are changes to the company’s policies or procedure related to the service being evaluated.[33]

Level 2 of STAR allows organizations to build off cloud-oriented certifications and standards. Many security and privacy audits and certifications are available for the organizations that choose to implement a third-party audit. Location, regulations and standards are the criteria for choosing the appropriate ones. Level 2 includes the following variations:

- STAR Attestation: For SOC 2
  The CSA STAR Attestation is a collaboration between CSA and the American Institute of Certified Public Accountants (AICPA) to provide guidelines for Certified Public Accountants (CPAs) to conduct Service Organization Control (SOC) 2 engagements using criteria from the AICPA (Trust Service Principles, AT 101) and the CSA Cloud Controls Matrix. The STAR Attestation provides strict third-party independent assessments of cloud providers. Attestation listings expire after one year unless updated.
- STAR Certification: For ISO/IEC 27001:2013
  The CSA STAR Certification is a strict third-party independent assessment of the security of a cloud service provider. This certification leverages the requirements of the ISO/IEC 27001:2013 management system standard together with the CSA Cloud Controls Matrix.

Certification certificates comply with ISO/IEC 27001 protocol and expire after three years unless updated.

- C-STAR: For the Greater China Market
  The CSA C-STAR Assessment is a robust third-party independent security assessment of a cloud service provider for the Greater China market that harmonizes 5CSA best practices with Chinese national standards. C-STAR leverages the requirements of the GB/T 22080-2008 management system standard together with the CSA Cloud Controls Matrix, plus 29 related controls selected from GB/T 22239- 2008 and GB/Z 28828-2012. Certification certificates expire after three years unless updated. [35]

5.3.3 ISO

The International Organization for Standardization (ISO) is an independent, non-governmental international organization that develops and publishes standards for a wide range of industries and sectors. Founded in 1947 and based in Geneva, Switzerland, ISO has published over 25,000 international standards covering almost all aspects of technology and manufacturing. It has over 800 technical committees (TCs) and subcommittees (SCs) to take care of standards development. ISO aims to facilitate international trade by providing common standards that ensure quality, safety, efficiency, and interoperability of products and services across different countries. Implementing ISO standards can help organizations improve their efficiency, reduce costs, manage risks, and enhance customer satisfaction. Standards also promote international trade by ensuring that products and services meet the same specifications and quality levels globally.[36]

Popular ISO Standards:

- *ISO 14001:* focuses on helping organizations improve their environmental performance.
- *ISO 45001:* aims at reducing workplace risks and creating safer working conditions.
- *ISO/IEC 27001:* outlines best practices for managing sensitive company information to keep it secure.
- *ISO 27017:* This standard is part of the ISO/IEC 27000 family of standards that provide best practice recommendations on information security management. Is a security standard developed for cloud service providers and cloud service users to make a safer cloud-based environment and reduce threats.
- *ISO 27002:* It is part of the ISO/IEC 27000 family of standards as well and it provides guidelines for information security controls to be used for information security management systems (ISMS) implementation and maintenance.

In this thesis, we will dive into ISO 27017 and ISO 27002:2022 [37,38]

5.3.3.1 ISO 27017

ISO/IEC 27017 standard was developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) and released in December 2015. Is considered as part of the broader ISO/IEC 27000 standard, which focuses on ISMS. ISO/IEC 27017 provides guidance for security controls for usage and provisioning of cloud services to both cloud

service providers (CSPs) and cloud customers. with guidance on how to manage and mitigate cloud-specific risks. [39,40,41,42]

ISO/IEC 27017 provides instructions for information security controls, for both cloud service providers and cloud service customers, applicable to the usage of cloud services by providing:

- Implementation guidance for relevant controls in addition to the ones already specified in ISO/IEC27002,
- implementation guidance for controls that are specially related to cloud services. [40]

ISO/IEC 27017 structure according to ISO published standard consists of:

1.Information Security Policies: Focuses on information security, to ensure they meet cloud-specific needs.

2.Organization of Information Security: Refers to internal organization, roles and responsibilities, segregation of duties, and contact with authorities relevant to cloud security.

3.Human Resource Security: Includes screening, terms and conditions of employment, and security awareness training during employment.

4.Asset Management: Covers inventory and ownership of assets, assets maintenance, assets labeling, media handling and return of assets specific to the cloud environment.

5.Access Control: Details about access control policies, user access management, and user responsibilities, emphasizing the importance of secure log-on procedures and the management of privileged access.

6.Cryptography: Specifies cryptographic controls and key management for securing data in cloud environments.

7.Physical and Environmental Security: Refers to physical security and equipment protection, cabling security, assets removal and disposal to safeguard physical assets and data, unattended user equipment handling and clear desk/clear screen policy.

8.Operations Security: Covers procedures and responsibilities, capacity management, and change management to ensure ongoing security in operational processes.

9.Communications Security: Focuses on network security management and the integrity of information transfer procedures (electronic messaging, non-disclosure agreements).

10.System Acquisition, Development, and Maintenance: Addresses secure development and system change control to manage vulnerabilities in cloud services.

11.Supplier Relationships: Outlines the need for security in supplier agreements and the management of supplier relationships.

12.Information Security Incident Management: Details incident reporting, response mechanisms, learning from incidents and collecting evidence to improve security practices.

13.Information Security Aspects of Business Continuity Management: Discusses planning for information security continuity and ensuring redundancy.

14.Compliance: Focuses on adhering to legal, regulatory, and contractual requirements, with particular attention to the protection of personally identifiable information (PII). [40]

According to ISO and Tuv Sud blog, ISO/IEC 27017 standard's benefits include

1.Enhanced Security: By implementing the guidelines and controls in ISO/IEC 27017, organizations can strengthen their cloud security posture, reducing the risk of data breaches and other security incidents.

2.Improved Trust: Adhering to ISO/IEC 27017 demonstrates a commitment to security, helping to build trust with customers, partners, and stakeholders. This can be a competitive advantage for CSPs looking to differentiate themselves in the market.

3.Regulatory Compliance: Following ISO/IEC 27017 can help organizations meet the requirements of various data protection regulations, reducing the risk of legal penalties and reputational damage.

4.Clear Responsibilities: The shared responsibility model outlined in ISO/IEC 27017 helps both CSPs and cloud customers understand their respective roles in securing cloud services, promoting better collaboration and communication.

5.Continuous Improvement: ISO/IEC 27017 encourages organizations to regularly assess and improve their cloud security practices, ensuring that they remain effective in the face of new and emerging threats. [42]

5.3.3.2 ISO 27002:2022

ISO/IEC 27002:2022 provides best practice recommendations on information security controls for use by those responsible for initiating, implementing, and maintaining information security management systems. The 2022 version includes updates to reflect the current cybersecurity landscape, including new controls for cloud security. [41, 43]

This document provides a reference set of generic information security controls including implementation guidance. This document is designed to be used by organizations:

- within the context of an information security management system (ISMS) based on ISO/IEC 27001,
- for developing organization-specific information security management guidelines,
- for implementing information security controls based on internationally recognize [43]

ISO/IEC 27002 structure according to ISO published standard consists of:

1. Organizational Controls

1.1 Information Security Policies: Highlights the suitability and effectiveness of management guidance and support for information security in alliance with business and legal requirements.

1.2 Information security roles and responsibilities: To protect information within the organization. To establish a well-defined structure for the deployment, execution, and oversight of information security within the organization.

1.3 Segregation of duties: Aims to protect against the risk of deception, errors and against information security controls violation.

1.4 Management responsibilities: For identifying and handling information security risks and protecting organization's assets. To ensure management and all personnel are aware of their role, information security responsibilities.

1.5 Contact with authorities: To ensure appropriate kind of information is exchanged between the organization and relevant legal, regulatory and supervisory authorities.

1.6 Contact with special interest groups: To guarantee that information is shared and communicated properly in accordance with information security guidelines.

1.7 Threat intelligence: To raise awareness of the organization's threat landscape, enabling the implementation of suitable mitigation measures.

1.8 Information security in project management: To make sure that information security risks associated with projects and deliverables are properly managed throughout the entire project life cycle.

1.9 Inventory of information and other associated assets: To determine the organization's data and other associated assets to preserve their information security and assign appropriate ownership.

1.10 Acceptable use of information and other associated assets: To guarantee that information and related assets are safeguarded, utilized responsibly, and handled correctly.

1.11 Return of assets: To secure the organization's assets during transitions such as employment changes, contract conclusions, or agreement terminations.

1.12 Classification of information: To ensure that information is identified, and its protection requirements are understood based on its significance to the organization.

1.13 Labeling of information: To aid in communicating information classification and to support the automation of processing and managing information.

1.14 Information transfer: To protect the security of information when it is being shared within the organization or with external parties.

1.15 Access control: To ensure that access to information and related assets is granted only to authorized individuals and to prevent unauthorized access.

1.16 Identity management: To enable the unique identification of individuals and systems that access the organization's information and assets, facilitating the proper allocation of access rights.

1.17 Authentication information: To ensure reliable authentication of entities and to prevent authentication failures.

1.18 Access rights: To define and authorize access to information and assets based on the organization's business needs.

1.19 Information security in supplier relationships: To ensure that an agreed level of information security is upheld in relationships with suppliers.

1.20 Addressing information security within supplier agreements: To maintain the established level of information security within supplier relationships.

1.21 Managing information security in the ICT supply chain: To uphold the agreed information security standards in supplier relationships.

1.22 Monitoring, review and change management of supplier services: To ensure that information security and service delivery are aligned with supplier agreements.

1.23 Information security for use of cloud services: To define and manage information security measures for the utilization of cloud services.

1.24 Information security incident management planning and preparation: To facilitate a swift, effective, and organized response to information security incidents, including communication about security events.

1.25 Assessment and decision on information security events: To ensure the effective classification and prioritization of information security events.

1.26 Response to information security incidents: To provide a prompt and effective reaction to information security incidents.

1.27 Learning from information security incidents: To minimize the chances or impact of future security incidents.

1.28 Collection of evidence: To consistently and effectively manage evidence related to information security incidents for potential disciplinary and legal actions.

1.29 Information security during disruption: To safeguard information and related assets during periods of disruption.

1.30 ICT readiness for business continuity: To guarantee the availability of the organization's information and assets during disruptions.

1.31 Legal, statutory, regulatory and contractual requirements: To ensure adherence to information security-related legal, statutory, regulatory, and contractual obligations.

1.32 Intellectual property rights: To comply with legal, statutory, regulatory, and contractual obligations concerning intellectual property rights and the use of proprietary products.

1.33 Protection of records: To meet legal, statutory, regulatory, and contractual requirements, as well as societal expectations, related to the safeguarding and accessibility of records.

1.34 Privacy and protection of PII: To comply with information security aspects of legal, statutory, regulatory, and contractual requirements regarding the protection of Personally Identifiable Information (PII).

1.35 Independent review of information security: To confirm the ongoing relevance, adequacy, and effectiveness of the organization's information security management approach.

1.36 Compliance with policies, rules and standards for information security: To ensure that information security practices align with the organization's policies, rules, and standards.

1.37 Documented operating procedures: To ensure information processing facilities operate correctly and securely.

2. People Controls

2.1 Screening: To verify that all personnel are qualified and appropriate for their roles and continue to meet eligibility and suitability requirements throughout their employment.

2.2 Terms and conditions of employment: To ensure that personnel understand their information security obligations associated with their roles.

2.3 Information security awareness, education and training: To ensure that personnel and relevant parties are informed of and adhere to their information security duties.

2.4 Disciplinary process: To clarify the repercussions of violating information security policies and to discourage and appropriately handle violations by personnel and other relevant parties.

2.5 Responsibilities after termination or change of employment: To safeguard the organization's interests during employment changes or contract terminations.

2.6 Confidentiality or non-disclosure agreements: To ensure that information accessed by personnel or external parties remains confidential.

2.7 Remote working: To protect information security when personnel are working outside the organization's premises.

2.8 Information security event reporting: To facilitate prompt, consistent, and effective reporting of information security events identified by personnel.

3. Physical Controls

3.1 Physical security perimeters: To block unauthorized physical access, prevent damage, and avoid interference with the organization's information and assets.

3.2 Physical entry: To ensure that only authorized individuals gain physical access to the organization's information and assets.

3.3 Securing offices, rooms and facilities: To prevent unauthorized access, damage, and interference with information and assets within offices, rooms, and facilities.

3.4 Physical security monitoring: To identify and discourage unauthorized physical access.

3.5 Protecting against physical and environmental threats: To avert or lessen the impact of incidents stemming from physical and environmental hazards.

3.6 Working in secure areas: To safeguard information and assets from harm and unauthorized access by personnel in secure areas.

3.7 Clear desk and clear screen: To minimize the risks of unauthorized access, loss, or damage to information on desks, screens, and other accessible locations both during and outside of working hours.

3.8 Equipment siting and protection: To lower the risks associated with physical and environmental threats, as well as unauthorized access and damage.

3.9 Security of assets off-premises: To prevent loss, damage, theft, or compromise of devices used off-site and to avoid disruptions to the organization's operations.

3.10 Storage media: To ensure that information on storage media is disclosed, modified, removed, or destroyed only with proper authorization.

3.11 Supporting utilities: To prevent information loss, damage, compromise, or operational interruptions due to the failure or disruption of utilities.

3.12 Cabling security: To prevent loss, damage, theft, or compromise of information and assets, and to avoid operational interruptions related to power and communication cabling.

3.13 Equipment maintenance: To prevent loss, damage, theft, or compromise of information and assets, and to avoid operational interruptions due to insufficient maintenance.

3.14 Secure disposal or reuse of equipment: To prevent the unintended release of information from equipment that is being disposed of or repurposed.

4. Technological Control

4.1 User endpoint devices: To safeguard information from risks associated with using user endpoint devices.

4.2 Privileged access rights: To ensure that only authorized users, software components, and services have privileged access rights.

4.3 Information access restriction: To allow only authorized access and prevent unauthorized access to information and related assets.

4.4 Access to source code: To avoid unauthorized functionality, prevent unintentional or malicious changes, and maintain the confidentiality of valuable intellectual property.

4.5 Secure authentication: To securely verify the identity of users or entities when granting access to systems, applications, and services.

4.6 Capacity management: To ensure that the necessary capacity for information processing, human resources, offices, and other facilities is available.

4.7 Protection against malware: To protect information and related assets from malware.

4.8 Management of technical vulnerabilities: To prevent the exploitation of technical vulnerabilities.

4.9 Configuration management: To ensure that hardware, software, services, and networks operate correctly with the necessary security settings, and to prevent unauthorized or incorrect configuration changes.

4.10 Information deletion: To prevent unnecessary exposure of sensitive information and comply with legal, statutory, regulatory, and contractual requirements for deleting information.

4.11 Data masking: To minimize the exposure of sensitive data, including PII, and comply with legal, statutory, regulatory, and contractual obligations.

4.12 Data leakage prevention: To detect and prevent unauthorized disclosure and extraction of information by individuals or systems.

4.13 Information backup: To enable the recovery of data or systems in the event of loss.

4.14 Redundancy of information processing facilities: To ensure the continuous operation of information processing facilities.

4.15 Logging: To record events, provide evidence, ensure the integrity of log information, prevent unauthorized access, identify security events that could lead to incidents, and support investigations.

4.16 Monitoring activities: To detect unusual behavior and potential information security incidents.

4.17 Clock synchronization: To enable the correlation and analysis of security events and other recorded data, and support investigations into security incidents.

4.18 Use of privileged utility programs: To ensure that utility programs do not compromise system and application controls for information security.

4.19 Installation of software on operational systems: To maintain the integrity of operational systems and prevent the exploitation of technical vulnerabilities.

4.20 Network security: To protect information within networks and its supporting processing facilities from being compromised via the network.

4.21 Security of network services: To ensure the secure use of network services.

4.22 Segregation of networks: To divide the network into secure boundaries and control traffic between them based on business needs.

4.23 Web filtering: To protect systems from malware and prevent access to unauthorized web resources.

4.24 Use of cryptography: To ensure that cryptography is used effectively to protect the confidentiality, authenticity, or integrity of information, considering business needs and relevant legal, statutory, regulatory, and contractual requirements.

4.25 Secure development life cycle: To integrate information security into the design and implementation of software and systems throughout the development life cycle.

4.26 Application security requirements: To identify and address all security requirements when developing or acquiring applications.

4.27 Secure system architecture and engineering principles: To design, implement, and operate information systems securely within the development life cycle.

4.28 Secure coding: To write software securely, reducing potential security vulnerabilities.

4.29 Security testing in development and acceptance: To verify that security requirements are met when deploying applications or code to the production environment.
4.30 Outsourced development: To ensure that required information security measures are implemented in outsourced system development.

4.31 Separation of development, test, and production environments: To identify and implement the necessary level of separation between these environments to prevent issues in production.

4.32 Change management: To maintain information security during changes.

4.33 Test information: To ensure the relevance of testing and protect operational information used for testing.

4.34 Protection of information systems during audit testing: To minimize the impact of audits and other assurance activities on operational systems and business processes. [43]

Each category consists of guidance statements. All the above and more details are listed in ISO 27002:2022 standard. [43]

Achieving ISO/IEC 27002 certification offers numerous benefits for organizations, given its global recognition and respect. Some of the key advantages of complying with this standard include:

1.Enhanced Security Posture: Adhering to ISO/IEC 27002 guidelines enables organizations to implement strong information security controls that improve the protection of critical assets and data, helping to prevent data breaches and mitigate various security threats.

2.Compliance with Legal and Regulatory Requirements: ISO/IEC 27002 offers a framework that aids organizations in meeting legal, regulatory, statutory, and contractual requirements for information security, with a strong focus on complying with data protection regulations.

3.Improved Risk Management: The standard provides guidelines for effectively identifying and addressing information security risks, enabling organizations to minimize vulnerabilities and enhance their risk management practices. By performing a risk assessment, organizations can pinpoint potential threats and weaknesses within their information assets, allowing them to establish suitable controls for better managing these risks. This approach leads to more refined risk management processes and a more precise risk assessment.

4.Increased Customer Trust: Adhering to globally recognized security standards can boost customer confidence and trust by showcasing a strong commitment to safeguarding sensitive information. Additionally, it can strengthen the organization's visibility in the marketplace, highlighting its dedication to high security practices.

5.Operational Efficiency: Adopting standardized security controls can optimize processes, reduce redundancies, and enhance overall operational efficiency through the establishment of clear security protocols. This strategy not only deepens knowledge of information security practices but also refines the implementation of control policies.

6.Support for Continuous Improvement: ISO/IEC 27002 advocates for the regular review and updating of information security practices, fostering ongoing improvement and adaptation to emerging security threats. This approach can also lead to increased employee productivity. [43,44,45]

5.4 MITRE ATT&CK

Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK) is a knowledge base, developed by MITRE, is globally accessible and consists of tactics and techniques based on real-world observations. It is especially beneficial in cloud environments as it gathers and analyzes attacker's behavior and identifies potential weaknesses. Organizations leverage MITRE ATT&CK to improve their detection and response strategies by mapping possible attack pathways and strengthening their defenses accordingly. ATT&CK includes 3 categories: ATT&CK for Enterprise, ATT&CK for Mobile and Att&ck for Industrial Control Systems (ICS). ATT&CK for Enterprise covers attackers' behavior against enterprise IT networks and cloud, and ATT&CK for Mobile, focuses on attackers' behavior against mobile devices.On the other hand, MITRE ATT&CK for ICS is designed to reflect the tactics, techniques, and procedures (TTPs) used by adversaries targeting industrial control systems and assets. [46,47]

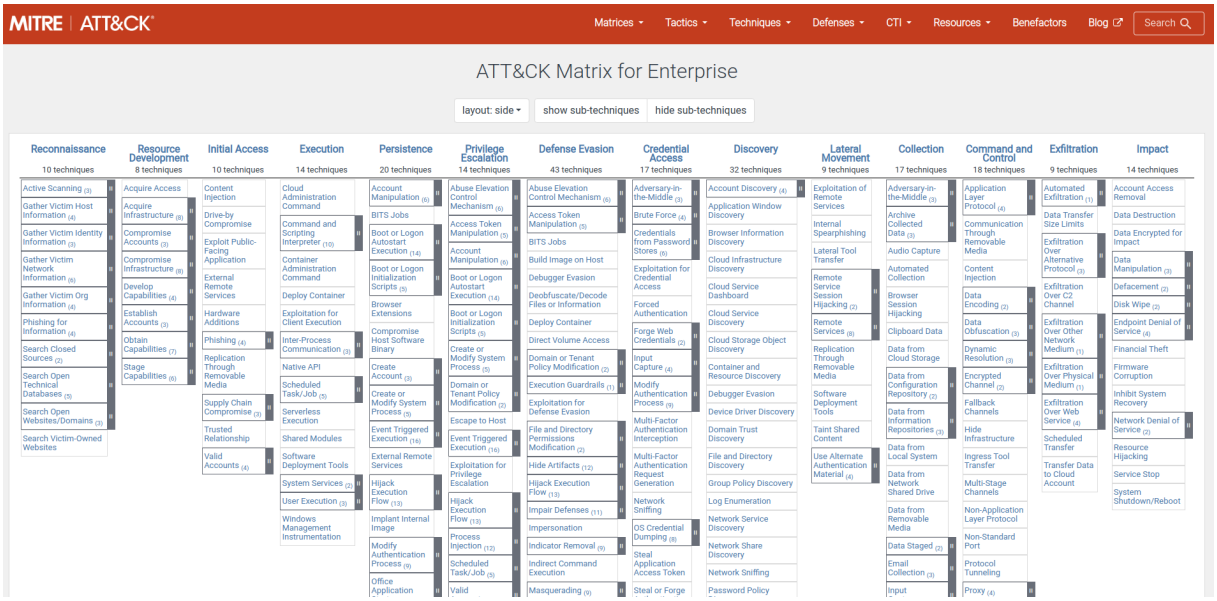

Image 5.3: ATT&CK Matrix for Enterprise [48]

5.4.1 Key Components of MITRE ATT&CK:

1.Tactics: Tactics represent the goals an adversary is trying to achieve at different phases in an attack. For example, tactics might include gaining initial access, credential access, discovery, lateral movement, etc. Tactics are the "why" behind an attacker's actions. In the following table, tactics are listed per category. [46]

Table 5.1: List of Tactics [48]

Tactic	**Enterprises**	**Mobile**	**ICIS**
Initial Access	●	●	●
Execution	●	●	●
Persistence	●	●	●
Privilege Escalation	●	●	●
Defense Evasion	●	●	-
Evasion	-	-	●
Credential Access	●	●	-
Discovery	●	●	●
Lateral Movement	●	●	●
Collection	●	●	●
Command and Control	●	●	●
Exfiltration	●	●	-
Impact	●	●	●
Reconnaissance	●	-	-
Resource Development	●	-	-
Inhibit Response Function	-	-	●
Impair Process Control	-	-	●

2. Techniques: Techniques represent the methods attackers use to achieve their goals. For example, under the tactic of "Initial Access," a technique might be "Phishing" or “Content Injection”. Techniques describe the "how" an attacker accomplishes their goals. The image below illustrates some techniques.

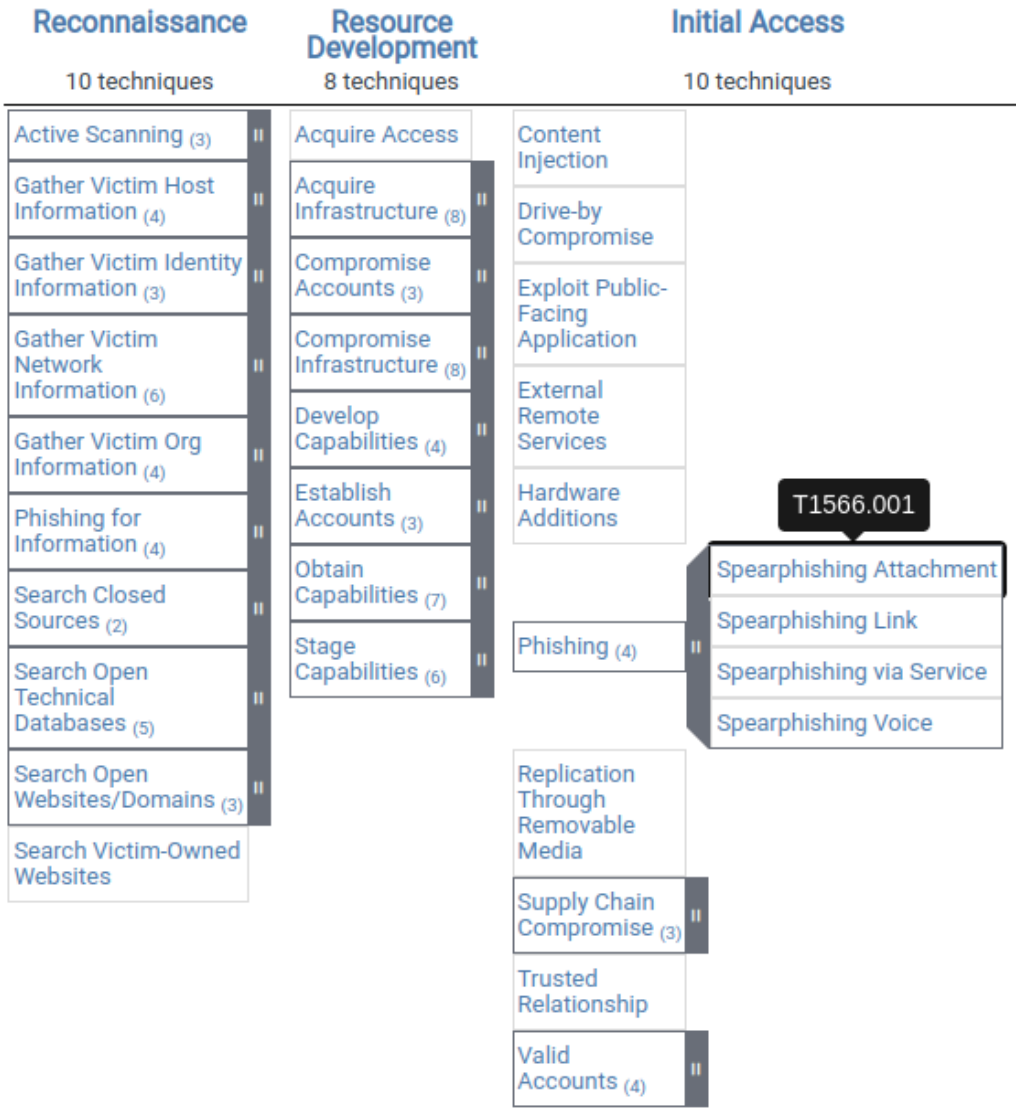

Image 5.4: Techniques [48]

3.Sub-Techniques: Sub-techniques provide additional specifics on how a specific action might be carried out under each technique. For example, under the "Phishing" technique, there might be sub-techniques like "Spearphishing via Service" or "Spearphishing Voice." In the following image, all Phishing sub-techniques are listed.

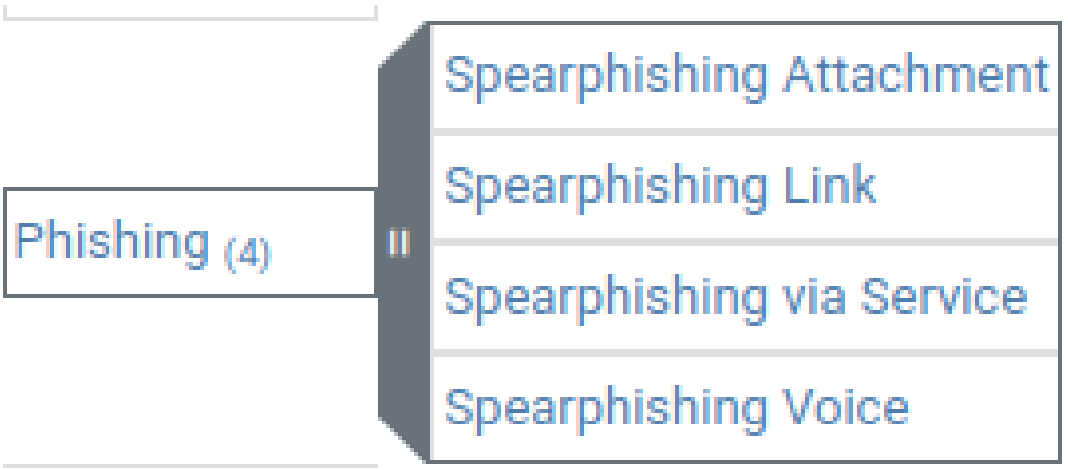

Image 5.5: Phishing Sub-Techniques [48]

Within each domain are platforms, which may be an operating system or an application (e.g. Microsoft Windows). Techniques and sub-techniques can apply to multiple platforms.

4. Procedures: Procedures describe in detail the specific actions taken by threat actors when executing a technique or sub-technique. These are often based on real-world examples. [48]

S0476	Valak	Valak has been delivered via spearphishing e-mails with password protected ZIP files.[231]
S0670	WarzoneRAT	WarzoneRAT has been distributed as a malicious attachment within an email.[248][69]
G0112	Windshift	Windshift has sent spearphishing emails with attachment to harvest credentials and deliver malware.[249]
G0090	WIRTE	WIRTE has sent emails to intended victims with malicious MS Word and Excel attachments.[250]

Image 5.6: Procedures [48]

5.4.2 Mitre ATT&CK Use Cases

- Threat Intelligence: ATT&CK provides cyber security analysts information that they can structure, compare, and analyze to identify attackers' behavior and based on that information, they can improve decision-making procedures.
- Detection and Analytics: The ATT&CK framework enables cybersecurity teams to create analytics designed to identify the techniques used by attackers. By leveraging ATT&CK, security professionals can anticipate and map out potential adversary actions within their systems, enhancing their capacity to detect, respond to, and mitigate threats. There are several valuable sources available for analysts to detect techniques:
- Process, process command line monitoring, file and registry monitoring are usually collected by Sysmon, Windows Event Logs, and many EDR platforms.
- Authentication logs, collected from the domain controller via Windows Event Logs.
- Packet capture, especially east/west capture such as that collected between hosts and enclaves inside the network by sensors.
- Adversary Emulation and Red Teaming: Adversary emulation is a red teaming approach that replicates a specific threat to an organization by blending in threat intelligence to guide the red team’s actions and behavior. The purpose is to allow organizations to evaluate their defenses and uncover vulnerabilities. First, the Adversary emulation team designs scenarios to test particular elements of an adversary's TTPs and then the red team executes these scenarios within a target network to assess the effectiveness of the organization’s defenses against the simulated threat.
- Assessment and Engineering: The ATT&CK can be utilized to evaluate an organization’s defensive capabilities. It can also be used as a guide for engineering decisions, such as selecting appropriate tools and deciding on logging strategies. ATT&CK assessments play a critical role in a broader strategy to supply security engineers and architects with actionable information, supporting threat-informed security enhancements:
- Evaluation of the alignment of current defenses with the techniques and adversaries outlined in ATT&CK.
- Pinpoint the most critical gaps in existing security measures.
- Adjust current defenses or implement new solutions to address those gaps effectively. [47,49]

5.5 AWS Foundation Security Best Practices Standard

The AWS Foundational Security Best Practices (FSBP) standard comprises a series of controls designed to identify instances where AWS accounts and resources do not align with established security best practices. This standard enables ongoing assessment of all AWS accounts and workloads, helping swiftly pinpoint areas where security practices may need improvement. It offers specific, actionable recommendations to enhance and sustain an organization's security posture. These controls cover security best practices for resources across various AWS services. Additionally, each control is categorized according to the specific security function it addresses. [50]
According to official AWS documentation and specifically the AWS Security Hub, controls per AWS service that apply to the FSBP standard are

Account.1: The AWS account should include security contact details.

ACM.1: Certificates from ACM or imported into ACM must be renewed periodically.

ACM.2: ACM-managed RSA certificates should use keys that are at least 2,048 bits in length.

APIGateway.1: Enable execution logging for REST and WebSocket APIs in API Gateway.

APIGateway.2: API Gateway REST API stages should utilize SSL certificates for backend validation.

APIGateway.3: Enable AWS X-Ray tracing for REST API stages in API Gateway.

APIGateway.4: API Gateway should be linked with a Web ACL from AWS WAF.

APIGateway.5: Cache data in API Gateway REST APIs should be encrypted when stored.

APIGateway.8: Specify an authorization method for all routes in API Gateway.

APIGateway.9: API Gateway V2 stages should have access logging enabled.

AppSync.2: Enable field-level logging in AWS AppSync.

AppSync.5: AppSync GraphQL APIs should not rely on API keys for authentication.

Athena.4: Logging should be enabled for Athena workgroups.

AutoScaling.1: Auto Scaling groups that are connected to load balancers should rely on ELB health checks.

AutoScaling.2: Auto Scaling groups should span multiple Availability Zones.

AutoScaling.3: EC2 instances launched by Auto Scaling should be configured to require Instance Metadata Service Version 2 (IMDSv2).

Autoscaling.5: EC2 instances launched using Auto Scaling groups should not have Public IP addresses.

AutoScaling.6: Auto Scaling groups should employ multiple instance types across multiple Availability Zones.

AutoScaling.9: Auto Scaling groups should be configured to use EC2 launch templates.

Backup.1: Recovery points managed by AWS Backup should be encrypted when stored.

CloudFront.1: CloudFront distributions should have a default root object specified.

CloudFront.3: Ensure that CloudFront distributions enforce encryption during data transmission.

CloudFront.4: Set up origin failover for CloudFront distributions.

CloudFront.5: CloudFront distributions should enable logging.

CloudFront.6: Enable AWS WAF for CloudFront distributions.

CloudFront.7: CloudFront distributions should use custom SSL/TLS certificates.

CloudFront.8: CloudFront should utilize SNI for handling HTTPS requests.

CloudFront.9: Traffic from CloudFront to custom origins should be encrypted.

CloudFront.10: Avoid using deprecated SSL protocols between CloudFront edge locations and custom origins.

CloudFront.12: Ensure CloudFront distributions do not reference non-existent S3 origins.

CloudFront.13: Origin access control should be used with CloudFront distributions.

CloudTrail.1: Enable CloudTrail with at least one multi-region trail, capturing both read and write management events.

CloudTrail.2: CloudTrail logs should be encrypted when stored.

CloudTrail.4: Log file validation should be activated for CloudTrail.

CloudTrail.5: CloudTrail logs should be integrated with CloudWatch Logs for real-time monitoring.

CodeBuild.1: Avoid including sensitive credentials in Bitbucket source repository URLs for CodeBuild projects.

CodeBuild.2: Do not store credentials in plain text in CodeBuild project environment variables.

CodeBuild.3: Enable encryption for CodeBuild S3 logs.

CodeBuild.4: CodeBuild project environments should be configured to support logging.

CodeBuild.7: Report group exports in CodeBuild should be encrypted when stored.

Config.1: Enable AWS Config and ensure that resource recording is performed using the service-linked role.

DataFirehose.1: Firehose delivery streams must have encryption enabled for data stored at rest.

DataSync.1: Ensure that logging is activated for DataSync tasks.

DMS.1: Database Migration Service replication instances should not be configured to allow public access.

DMS.6: Automatic minor version upgrades should be enabled for DMS replication instances.

DMS.7: Logging should be enabled for DMS replication tasks targeting the destination database.

DMS.8: Logging should be enabled for DMS replication tasks targeting the source database.

DMS.9: DMS endpoints should be configured to use SSL for connections.

DMS.10: Enable IAM authorization for DMS endpoints connecting to Neptune databases.

DMS.11: DMS endpoints for MongoDB should be set up with an authentication method.

DMS.12: TLS should be enabled for DMS endpoints connected to Redis OSS.

DocumentDB.1: Amazon DocumentDB clusters should have encryption enabled for data stored at rest.

DocumentDB.2: Amazon DocumentDB clusters must be configured with a sufficient backup retention period.

DocumentDB.3: Manual Amazon DocumentDB cluster snapshots should not be publicly accessible.

DocumentDB.4: Amazon DocumentDB clusters should have audit logs published to CloudWatch Logs.

DocumentDB.5: Deletion protection should be activated for Amazon DocumentDB clusters.

DynamoDB.1: DynamoDB tables should automatically adjust their capacity based on demand.

DynamoDB.2: Point-in-time recovery should be enabled for DynamoDB tables.

DynamoDB.3: DynamoDB Accelerator (DAX) clusters should have encryption enabled for data at rest.

DynamoDB.6: Enable deletion protection for DynamoDB tables.

DynamoDB.7: DynamoDB Accelerator clusters should use encryption for in-transit data.

EC2.1: Amazon EBS snapshots should not be configured for public access.

EC2.2: Default VPC security groups should block both inbound and outbound traffic.

EC2.3: Amazon EBS volumes attached to EC2 instances should be encrypted at rest.

EC2.4: Stopped EC2 instances should be terminated after a defined period.

EC2.6: Enable VPC flow logging in all VPCs.

EC2.7: Default encryption for EBS volumes should be activated.

EC2.8: EC2 instances should utilize Instance Metadata Service Version 2 (IMDSv2).

EC2.9: EC2 instances should not be assigned a public IPv4 address.

EC2.10: Amazon EC2 should utilize VPC endpoints created specifically for EC2 services.

EC2.15: EC2 subnets should not be automatically assigned public IP addresses.

EC2.16: Remove unused Network Access Control Lists (NACLs).

EC2.17: EC2 instances should avoid using multiple ENIs unless required.

EC2.18: Security groups should only allow unrestricted traffic on authorized ports.

EC2.19: Unrestricted access to high-risk ports should not be permitted by security groups.

EC2.20: Ensure both VPN tunnels for AWS Site-to-Site VPN connections remain active.

EC2.21: Network ACLs should block ingress from 0.0.0.0/0 to ports 22 or 3389.

EC2.23: EC2 Transit Gateways should not automatically accept VPC attachment requests.

EC2.24: Avoid using paravirtual EC2 instance types.

EC2.25: EC2 launch templates should not assign public IPs to network interfaces.

EC2.51: Client connection logging should be enabled for EC2 Client VPN endpoints.

ECR.1: Enable image scanning for private ECR repositories.

ECR.2: Tag immutability should be enabled for private ECR repositories.

ECR.3: At least one lifecycle policy should be configured for ECR repositories.

ECS.1: ECS task definitions should enforce secure networking and user configurations.

ECS.2: ECS services should not automatically assign public IPs.

ECS.3: ECS task definitions should not allow sharing the host's process namespace.

ECS.4: ECS containers should not be run with elevated privileges.

ECS.5: ECS containers should restrict root filesystem access to read-only mode.

ECS.8: Do not pass secrets as container environment variables.

ECS.9: Enable logging for ECS task definitions.

ECS.10: ECS Fargate services should operate on the latest Fargate platform version.

ECS.12: Enable Container Insights for ECS clusters.

EFS.1: Elastic File System (EFS) should use AWS KMS for encrypting file data at rest.

EFS.2: EFS volumes should be part of a backup plan.

EFS.3: EFS access points should enforce the root directory setting.

EFS.4: EFS access points should enforce a user identity.

EFS.6: Ensure EFS mount targets are not associated with public subnets.

EFS.7: EFS file systems should have automated backups enabled.

EKS.1: EKS cluster endpoints should be configured to prevent public access.

EKS.2: EKS clusters should run on a supported Kubernetes version.

EKS.3: Enable encryption for Kubernetes secrets within EKS clusters.

EKS.8: Ensure audit logging is enabled for EKS clusters.

ElastiCache.1: Automatic backups should be enabled for ElastiCache (Redis OSS) clusters.

ElastiCache.2: Auto minor version upgrades should be enabled for ElastiCache (Redis OSS) clusters.

ElastiCache.3: Enable automatic failover for ElastiCache (Redis OSS) replication groups.

ElastiCache.4: Ensure ElastiCache (Redis OSS) replication groups are encrypted at rest.

ElastiCache.5: Data in transit for ElastiCache (Redis OSS) replication groups should be encrypted.

ElastiCache.6: Redis AUTH should be enabled for earlier versions of ElastiCache (Redis OSS) replication groups.

ElastiCache.7: Do not use default subnet groups for ElastiCache (Redis OSS) clusters.

Chapter 5

ElasticBeanstalk.1: Ensure that Elastic Beanstalk environments have enhanced health reporting activated.

ElasticBeanstalk.2: Managed platform updates should be enabled for Elastic Beanstalk environments.

ElasticBeanstalk.3: Elastic Beanstalk should send logs to CloudWatch Logs.

ELB.1: Application Load Balancers should redirect all HTTP requests to HTTPS.

ELB.2: Classic Load Balancers with SSL/HTTPS listeners should use AWS Certificate Manager-provided certificates.

ELB.3: Classic Load Balancer listeners should be configured to terminate HTTPS or TLS traffic.

ELB.4: Application Load Balancers should be configured to drop unnecessary HTTP headers.

ELB.5: Enable logging for Application and Classic Load Balancers.

ELB.6: Enable deletion protection for Application, Network, and Gateway Load Balancers.

ELB.7: Connection draining should be enabled for Classic Load Balancers.

ELB.8: Classic Load Balancers with SSL listeners should use strong predefined security policies.

ELB.9: Cross-zone load balancing should be enabled for Classic Load Balancers.

ELB.10: Classic Load Balancers should span across multiple Availability Zones.

ELB.12: Application Load Balancers should use the most restrictive desync mitigation mode.

ELB.13: Load Balancers should span across multiple Availability Zones.

ELB.14: Classic Load Balancers should use strict desync mitigation modes.

EMR.1: Amazon EMR cluster primary nodes should not be assigned public IP addresses.

EMR.2: Block public access settings should be enabled for Amazon EMR.

ES.1: Elasticsearch domains should have encryption enabled for data stored at rest.

ES.2: Elasticsearch domains should be configured to prevent public access.

ES.3: Enable encryption for data transmitted between Elasticsearch nodes.

ES.4: Elasticsearch domain error logs should be sent to CloudWatch Logs.

ES.5: Audit logging should be enabled for Elasticsearch domains.

ES.6: Elasticsearch domains should consist of at least three data nodes.

ES.7: At least three dedicated master nodes should be configured for Elasticsearch domains.

ES.8: Elasticsearch domains should enforce TLS encryption using the latest security policy.

EventBridge.3: Resource-based policies should be attached to custom EventBridge event buses.

FSx.1: FSx for OpenZFS volumes should be encrypted using KMS keys.

FSx.2: FSx for Lustre file systems should use KMS keys for encryption at rest.

FSx.5: FSx for OpenZFS file systems should have automatic backups enabled.

FSx.6: FSx for Lustre file systems should have automatic backups enabled.

FSx.8: FSx for OpenZFS file systems should enforce root directory mapping.

FSx.10: FSx for OpenZFS file systems should require root squash.

FSx.11: FSx for Lustre file systems should have root squash activated.

Glue.1: Glue Data Catalog tables should be encrypted at rest.

Glue.2: Glue crawlers should be set up with a security configuration.

Glue.3: Glue security configurations should require the encryption of CloudWatch Logs.

Glue.4: Glue security configurations should require the encryption of job bookmarks.

Glue.5: Glue development endpoints should be protected against public access.

Glue.6: Glue development endpoints should utilize IAM authentication.

Glue.7: Enable Glue job bookmark encryption.

Glue.8: Enable CloudWatch log encryption for Glue jobs.

GuardDuty.1: GuardDuty must be enabled to monitor AWS accounts.

GuardDuty.2: GuardDuty should include all organizational accounts.

IAM.1: Ensure there is at least one administrator IAM role in each AWS account.

IAM.2: Do not allow root accounts to be used for day-to-day operations.

IAM.3: Rotate IAM user access keys at least every 90 days to maintain security.

IAM.4: The IAM root user should not have any access keys.

IAM.5: Multi-factor authentication (MFA) should be enabled for all IAM users with a console login.

IAM.6: The root user should use hardware-based MFA for enhanced security.

IAM.7: Ensure that IAM user password policies enforce strong security configurations.

IAM.8: Deactivate or remove unused IAM user credentials.

IAM.21: Custom IAM policies should avoid allowing wildcard actions across AWS services.

Inspector.1: Activate Amazon Inspector to scan your EC2 instances for vulnerabilities.

Inspector.2: Enable Amazon Inspector scanning for Amazon ECR container images.

Inspector.3: Amazon Inspector should scan Lambda function code for security vulnerabilities.

Inspector.4: Lambda functions should undergo standard scanning using Amazon Inspector.

Kinesis.1: Kinesis data streams must be encrypted at rest to safeguard sensitive data.

KMS.1: Customer managed IAM policies should not permit decryption actions across all KMS keys.

KMS.2: Avoid inline IAM policies that grant decryption permissions on all KMS keys.

KMS.3: Prevent accidental deletion of AWS KMS keys to avoid data loss.

Lambda.1: Lambda function policies should block public access for security purposes.

Lambda.2: Lambda functions should operate on supported runtime environments.

Lambda.5: Ensure Lambda functions running within VPCs are spread across multiple Availability Zones.

Macie.1: Enable Amazon Macie to detect and protect sensitive data.

Macie.2: Use Macie's automated sensitive data discovery feature for continuous data protection.

MQ.2: Configure ActiveMQ brokers to stream audit logs to Amazon CloudWatch.

MQ.3: Ensure Amazon MQ brokers are set to apply minor updates automatically.

MSK.1: Encrypt data transmitted between MSK broker nodes to protect sensitive information.

Neptune.1: Neptune database clusters must have encryption at rest enabled.

Neptune.2: Enable audit logging for Neptune clusters and send logs to CloudWatch.

Neptune.3: Ensure Neptune cluster snapshots are not publicly accessible.

Neptune.4: Enable deletion protection for Neptune clusters to avoid accidental deletion.

Neptune.5: Activate automated backups for Neptune clusters to safeguard data.

Neptune.6: Neptune snapshots should be encrypted when stored at rest.

Neptune.7: Enable IAM database authentication for Neptune clusters.

Neptune.8: Ensure that tags for Neptune clusters are copied to snapshots.

NetworkFirewall.2: Ensure logging is enabled for AWS Network Firewall.

NetworkFirewall.3: Network Firewall policies should have at least one rule group attached.

NetworkFirewall.4: The default stateless action for full packets in Network Firewall policies should be either drop or forward.

NetworkFirewall.5: The default stateless action for fragmented packets should be drop or forward.

NetworkFirewall.6: Avoid having empty stateless rule groups in Network Firewall configurations.

NetworkFirewall.9: Enable deletion protection for AWS Network Firewalls.

Opensearch.1: Ensure encryption at rest is enabled for all OpenSearch domains.

Opensearch.2: OpenSearch domains should not be publicly accessible to prevent unauthorized access.

Opensearch.3: Enable encryption for data in transit between OpenSearch nodes.

Opensearch.4: Ensure OpenSearch domain error logs are sent to CloudWatch Logs.

Opensearch.5: Activate audit logging for OpenSearch domains to monitor access and actions.

Opensearch.6: OpenSearch domains should have at least three data nodes for redundancy.

Opensearch.7: Enable fine-grained access control for OpenSearch domains for enhanced security.

Opensearch.8: Enforce TLS encryption for OpenSearch domains using the latest security policies.

Opensearch.10: Ensure OpenSearch domains run the latest software version to receive updates and patches.

PCA.1: Disable AWS Private CA root certificate authority when not in use.

Route53.2: Enable logging for DNS queries in Route 53 public hosted zones.

RDS.1: Keep RDS snapshots private to prevent unauthorized access.

RDS.2: RDS DB instances should not allow public access, as configured in the PubliclyAccessible setting.

RDS.3: Enable encryption at rest for all RDS database instances.

RDS.4: Ensure RDS database and cluster snapshots are encrypted at rest.

RDS.5: Configure RDS DB instances with multi-AZ support for high availability.

RDS.6: Enable enhanced monitoring for RDS DB instances to track performance.

RDS.7: Activate deletion protection for RDS clusters to prevent accidental deletion.

RDS.8: Ensure deletion protection is enabled for RDS instances.

RDS.9: Enable logging for RDS DB instances and publish logs to CloudWatch.

RDS.10: Configure IAM authentication for RDS instances to manage access.

RDS.11: Enable automatic backups for RDS instances to secure data.

RDS.12: Enable IAM authentication for RDS clusters for better access control.

RDS.13: Enable automatic minor version upgrades for RDS instances.

RDS.14: Enable backtracking for Amazon Aurora clusters to quickly recover from errors.

RDS.15: RDS DB clusters should be set up for multi-AZ deployment for fault tolerance.

RDS.16: Ensure RDS clusters are configured to copy tags to snapshots.

RDS.17: Enable tag copying for RDS instances to propagate tags to snapshots.

RDS.18: RDS instances should be deployed within a Virtual Private Cloud (VPC).

RDS.19: Set up event notifications for critical cluster events in RDS.

RDS.20: Set up event notifications for critical RDS instance events.

RDS.21: Ensure RDS event notifications are configured for important database parameter group events.

RDS.22: RDS event notifications should be set up for significant database security group events.

RDS.23: RDS instances should not use the default database engine port.

RDS.24: Use a custom administrator username for RDS database clusters.

RDS.25: Ensure that RDS instances use a custom administrator username.

RDS.27: RDS DB clusters should have encryption at rest enabled.

RDS.34: Ensure Aurora MySQL clusters publish audit logs to CloudWatch Logs.

RDS.35: Enable automatic minor version upgrades for RDS clusters.

Redshift.1: Amazon Redshift clusters should not allow public access.

Redshift.2: Ensure Redshift clusters use encryption for data in transit.

Redshift.3: Enable automatic snapshots for Amazon Redshift clusters.

Redshift.4: Activate audit logging for Redshift clusters to monitor actions.

Redshift.6: Enable automatic major version upgrades for Amazon Redshift clusters.

Redshift.7: Redshift clusters should be configured to use enhanced VPC routing.

Redshift.8: Avoid using the default admin username for Redshift clusters.

Redshift.9: Redshift clusters should not rely on the default database name.

Redshift.10: Enable encryption at rest for Redshift clusters to protect stored data.

Redshift.15: Redshift security groups should limit ingress on the cluster port to trusted sources only.

S3.1: Enable block public access settings for all S3 general purpose buckets.

S3.2: S3 buckets should block public read access by default.

S3.3: Ensure that public write access is blocked for S3 buckets.

S3.5: Require the use of SSL for requests to access S3 general purpose buckets.

S3.6: S3 bucket policies should restrict access to specific AWS accounts.

S3.8: S3 buckets should have public access settings disabled.

S3.9: Enable server access logging for S3 general purpose buckets.

S3.12: Avoid using ACLs to manage access to S3 general purpose buckets.

S3.13: Set up lifecycle configurations for S3 general purpose buckets to manage data lifecycle.

S3.19: Block public access for all S3 access points.

SageMaker.1: Amazon SageMaker notebook instances should not have internet access directly.

SageMaker.2: Launch SageMaker notebook instances within a custom VPC for security.

SageMaker.3: SageMaker notebook users should not have root-level access.

SageMaker.4: SageMaker production endpoint variants should start with at least two instances.

SecretsManager.1: Enable automatic secret rotation in Secrets Manager.

SecretsManager.2: Ensure Secrets Manager secrets configured for rotation are successfully rotated.

SecretsManager.3: Remove any unused secrets from Secrets Manager.

SecretsManager.4: Rotate Secrets Manager secrets within a predefined number of days.

ServiceCatalog.1: Limit sharing of Service Catalog portfolios to within your AWS organization.

SQS.1: Enable encryption at rest for Amazon SQS queues to protect data.

SSM.1: EC2 instances should be managed using AWS Systems Manager.

SSM.2: Ensure EC2 instances managed by Systems Manager show as compliant after patch installations.

SSM.3: Verify compliance status for EC2 instances managed by Systems Manager associations.

SSM.4: SSM documents should not be shared publicly.

StepFunctions.1: Ensure logging is activated for Step Functions state machines.

Transfer.2: Do not use FTP protocol for Transfer Family server connections.

WAF.1: Enable logging for AWS WAF Classic global web ACLs.

WAF.2: Regional AWS WAF Classic rules should include at least one condition.

WAF.3: AWS WAF Classic regional rule groups should contain at least one rule.

WAF.4: Ensure regional web ACLs in AWS WAF Classic include at least one rule or rule group.

WAF.6: AWS WAF Classic global rules should include at least one condition.

WAF.7: AWS WAF Classic global rule groups should contain at least one rule.

WAF.8: Ensure global web ACLs in AWS WAF Classic include at least one rule or rule group.

WAF.10: AWS WAF web ACLs must contain at least one rule or rule group.

WAF.12: Ensure CloudWatch metrics are enabled for AWS WAF rules.

WorkSpaces.1: Encrypt user volumes for AWS WorkSpaces at rest.

WorkSpaces.2: Enable encryption at rest for AWS WorkSpaces root volumes. [50]

In the AWS security blog “AWS Security Reference Architecture: A guide to designing with AWS security services” the AWS Security Architecture is represented. [51]

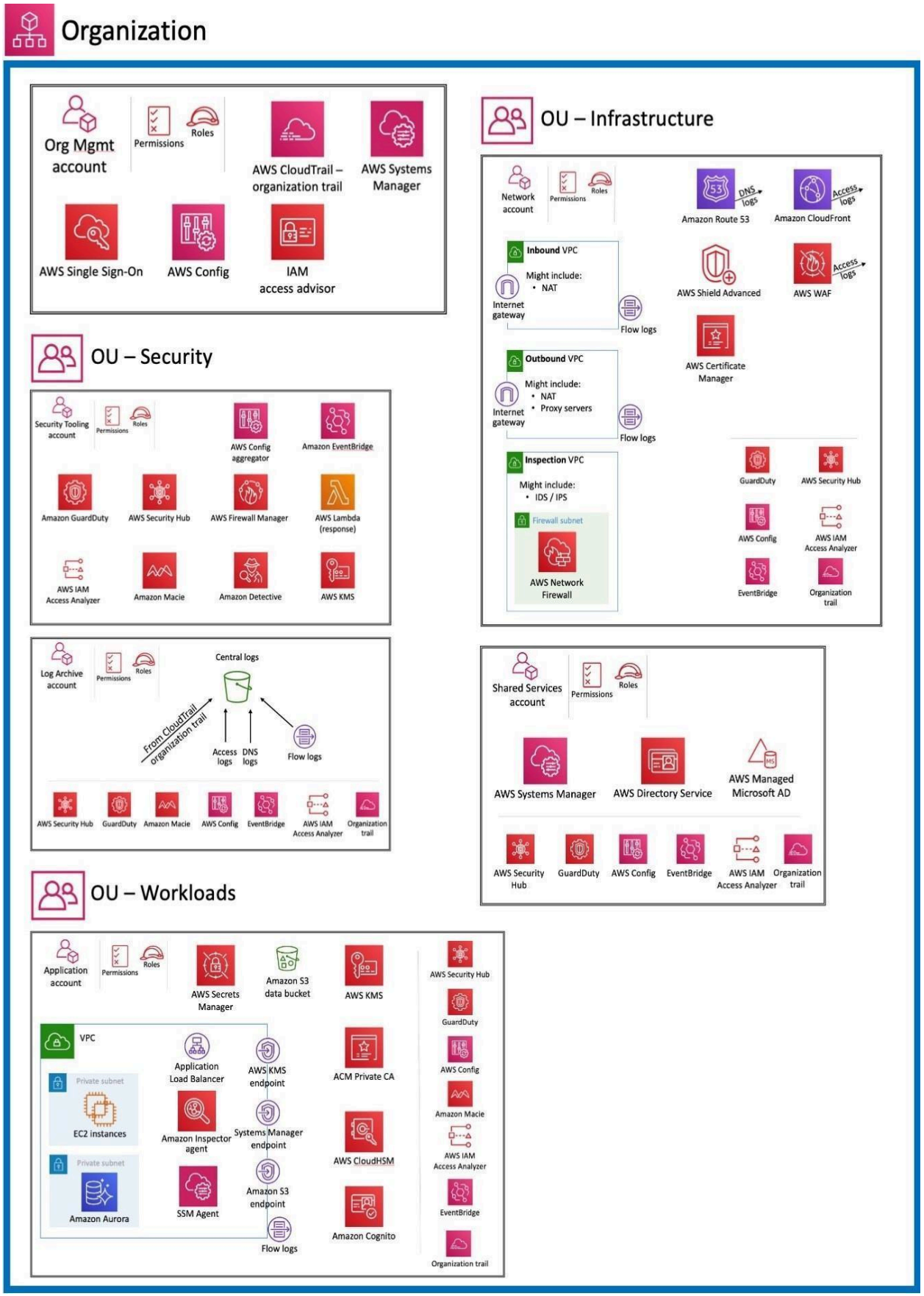

Image 5.7: The AWS Security Architecture [51]

5.6 Microsoft Cloud Security Benchmarks

The Microsoft Cloud Security Benchmark (MCSB) consists of guidance and detailed best practices and recommendations designed to enhance the security of data, and services across Azure and multi-cloud environments. Each control section provides guidance and strategies to assist organizations in effectively securing their Azure environments, covering a wide range of cloud security aspects, from network protection to compliance management. [52]

1.Network security (NS): Network Security focuses on securing and protecting network infrastructure within Azure. This includes measures to secure virtual networks, establish private connections, prevent and mitigate external threats, protect DNS, and secure communications within Azure environments. Key elements include:

- Network Controls: Use Azure Virtual Network to isolate resources and control traffic flow with network security groups (NSGs) and Azure Firewall.
- Protection from Network Attacks: Implement DDoS Protection, and secure Internet-facing applications with Azure Web Application Firewall.
- Network Security Monitoring: Use Azure Monitor, Network Watcher, and Azure Security Center for monitoring and logging network activity. [52, 53]

2.Identity Management (IM): Identity Management focuses on controls to establish secure identity and access mechanisms using identity and access management (IAM) systems. This includes the use of single sign-on, strong authentication methods, managed identities (including service principals for applications), conditional access, and monitoring for account anomalies. Important aspects include:

- Identity and Authentication: Enforce Multi-Factor Authentication (MFA) and manage identities using Azure Active Directory (Azure AD).
- Identity Protection: Use tools like Azure AD Identity Protection to detect and respond to suspicious activities.
- Access Management: Implement Role-Based Access Control (RBAC) to enforce the principle of least privilege. [52, 54]

3.Privileged Access (PA): Privileged Access pertains to protecting elevated access to an organization's tenant and resources. This involves implementing various controls to secure administrative accounts, and safeguard privileged access workstations from both deliberate and accidental risks. This section emphasizes managing and securing critical resources:

- Privileged Access Management: Use Privileged Identity Management (PIM) to oversee and control access to Azure resources.
- Administrative Access: Limit and monitor privileged access, enforce just-in-time access, and use Azure AD Conditional Access policies. [52, 55]

4.Data Protection (DP): Data Protection encompasses controls for safeguarding data. This includes discovering, classifying, protecting, and monitoring sensitive data assets using access controls, encryption, key management, and certificate management. The primary goal is to ensure the confidentiality, integrity, and availability of data:

- Data Classification and Encryption: Classify data and apply encryption in transit and at rest using Azure services.
- Data Loss Prevention (DLP): Use Azure Information Protection for data labeling and DLP policies to prevent unauthorized data sharing.
- Data Integrity and Isolation: Implement measures like Azure SQL Database encryption and Storage Service Encryption (SSE). [52, 56]

5.Asset Management (AM): Asset Management involves ensuring visibility and governance over organizational resources. This includes recommendations for security personnel permissions, securing access to asset inventories, and managing approvals for services and resources. The focus here is on identifying, managing, and tracking assets:

- Asset Inventory: Maintain an inventory of all Azure resources using tools like Azure Resource Graph and Azure Policy.
- Configuration Management: Use Azure Automation and Azure Policy to ensure resources are configured securely. [52, 57]

6.Logging and Threat Detection (LT): Logging and Threat Detection involves implementing controls to detect threats in cloud environments, as well as enabling, collecting, and storing audit logs for cloud services. This includes enabling detection, investigation, and remediation processes, generating high-quality alerts with native cloud threat detection, and centralizing security analysis using SIEM. Time synchronization and log retention are also part of this focus, which is on monitoring, logging, and detecting threats:

- Logging: Enable and centralized logging using Azure Monitor, Log Analytics, and Azure Activity Logs.
- Threat Detection: Use Azure Security Center and Microsoft Defender for Cloud to detect and respond to threats. [52, 58]

7. Incident Response (IR): Incident Response care related with preparation, detection and analysis. This involves using Azure services (such as Microsoft Defender for Cloud and Sentinel) and/or other cloud services to automate incident response processes. The focus is on preparing for and responding to security incidents:

- Incident Response Planning: Develop and regularly update incident response plans, using Azure Security Center's incident tracking.
- Detection and Response: Implement automation for incident response with Azure Sentinel and Logic Apps. [52, 59]

8.Posture and Vulnerability Management (PV): Posture and Vulnerability Management focuses on evaluating and enhancing cloud security. This includes vulnerability scanning, penetration testing, and remediation, as well as tracking, reporting, and correcting security configurations in cloud resources. The section deals with managing security posture and vulnerabilities:

- Security Posture Management: Regularly assess security posture using Azure Security Center and Azure Policy.
- Vulnerability Management: Use tools like Microsoft Defender for Cloud and Azure Security Benchmark to identify and remediate vulnerabilities. [52, 60]

9.Endpoint Security (ES): Endpoint Security covers controls for endpoint detection and response, including the use of tools and anti-malware services for endpoints within cloud environments. The focus is on securing endpoints in Azure:

- Endpoint Protection: Deploy Microsoft Defender for Endpoint to protect against malware and other threats.
- Access Controls: Implement Conditional Access policies to secure endpoint access. [50, 59]

10.Backup and Recovery (BR): Backup and Recovery involves implementing controls to ensure that data and configuration backups are conducted, validated, and protected across different service tiers. This section addresses the critical need for reliable data backup and recovery solutions:

- Backup Solutions: Use Azure Backup to create and manage backups for Azure VMs, databases, and other resources.
- Disaster Recovery: Implement Azure Site Recovery for business continuity and disaster recovery planning. [52, 62]

11.DevOps Security (DS): DevOps Security includes controls related to security engineering and operations within DevOps processes. This involves deploying critical security checks, such as security testing, before the deployment phase to ensure security throughout the DevOps lifecycle. The focus is on integrating security practices into DevOps workflows:

- Secure DevOps Practices: Use Azure DevOps and GitHub security features to integrate security into CI/CD pipelines.
- Code Security: Implement static analysis and other security testing in development pipelines. [52, 63]

12.Governance and Strategy (GS): Governance and Strategy provides guidelines for establishing a coherent security strategy and documented governance approach. This includes defining roles and responsibilities for cloud security functions. The focus is on establishing governance frameworks and aligning security with organizational strategy:

- Governance Framework: Use Azure Policy, Azure Blueprints, and Azure Security Center to enforce organizational policies.
- Compliance Management: Utilize compliance tools in Azure to ensure adherence to industry standards and regulations. [52, 64]

The image below represents a blueprint that deploys Azure services providing a secure, monitored, enterprise-ready architecture as it is displayed in Microsoft Learning section. [65]

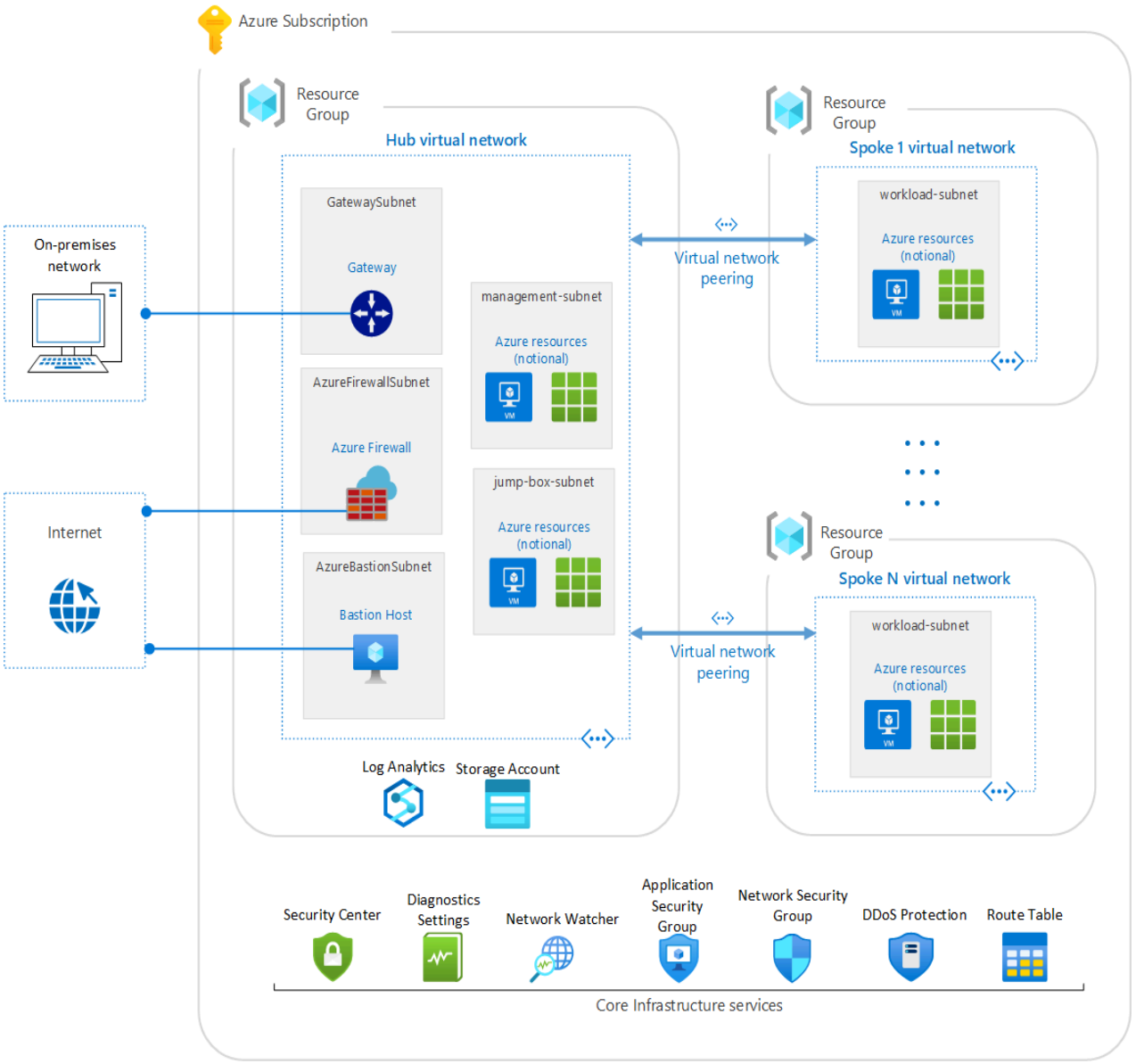

Image 5.8: Azure Security Benchmark Foundation blueprint [65]

5.7 Epilogue

In this chapter, cloud key security frameworks and standards were evaluated, highlighting their importance in safeguarding cloud infrastructures. By implementing these best practices, organizations can enhance their security posture, mitigate risks, and ensure compliance with industry regulations across diverse cloud platforms.

Chapter 6: Custom Cloud Security Framework for Greek SMEs

6.1 Introduction

This chapter focuses on the widely recognized frameworks ISO 27002:2022, AWS Foundational Security Best Practices Standard and CIS Amazon Web Services Benchmarks. Both provide essential guidelines for implementing effective security controls in cloud and hybrid environments, helping organizations manage risks, safeguard data, and meet regulatory requirements. These frameworks are especially valuable for small to medium-sized businesses looking to develop a strong cloud security posture. For the purposes of this thesis, the focus will be on infrastructure implementation in AWS which will be examined in detail. The policies outlined in this chapter are designed to reference both ISO 27002:2022 and AWS best practices, ensuring a comprehensive approach to cloud security tailored to the AWS environment.

6.2 Requirements and Key Steps

6.2.1 Policy Key Points

Taking under consideration both ISO 27002:2022, AWS best security practices and CIS Amazon Web Services Benchmarks, the essential focus areas that an organization or project must adhere to in order to maintain a robust security posture, shall include the following categories:

- *Access Control and Management:* Establish strict guidelines governing system access, including multi-factor authentication, the least privilege model, role-based access, and the use of groups and policies.
- *Data Security:* Implement encryption protocols and set rules for data classification and retention to safeguard sensitive information during transmission and storage.
- *Data Backup and Recovery:* Regularly backup data and perform tests on disaster recovery plans to ensure resilience.
- *Network Security:* Secure network configurations by using segmentation, access control lists (ACLs), and firewalls to protect vital systems and resources.
- *Incident Detection and Response:* Set up mechanisms for detecting threats, keep detailed logs, and have a defined response plan in place that includes roles, responsibilities, and escalation paths for handling security incidents.
- *Monitoring and Logging:* Deploy comprehensive monitoring and logging systems to enable timely identification of security threats.
- *Asset Management:* Maintain an up-to-date inventory of all assets, including AWS resources, to ensure full visibility and control.
- *Supplier Relationships & Third-Party Risks*: Evaluate and mitigate risks associated with third-party providers, ensuring they adhere to appropriate security standards.
- *Compliance and Audit:* Ensure adherence to relevant regulations and perform regular audits to verify the security posture.

- *Personnel Policy:* Outline key expectations for employees, contractors, and anyone with access to sensitive information, ensuring that they are trained, informed of their responsibilities, and contribute to an overall secure environment. [43, 50, 51]

6.2.2 Applying MoSCoW Prioritization

The MoSCoW prioritization technique, developed in 1994 by Dai Clegg and originally introduced as part of the Dynamic Systems Development Method (DSDM) in 2002. MoSCoW technique is a commonly used approach for handling requirements across multiple areas, such as information security and cloud computing. This method is particularly useful in policy and control development, ensuring that the most vital security components are prioritized, especially when resources and time are limited. This method categorizes tasks and features into four distinct groups to streamline decision-making and ensure that resources are allocated efficiently to meet project goals. [66,67]
The groups, as the acronym MoSCoW states, are

- Must have
- Should have
- Could have
- Won't have

Must Have: These are the critical requirements or features that are essential for a project's success or a security policy. Without these, the project would fail to achieve its fundamental objectives. They are necessary for the system to operate effectively and fulfill its primary functions. Prioritizing these ensures that the project meets its core deliverables. In the context of a security policy, these items refer to indispensable controls that mitigate significant security risks, such as data encryption, identity management, and access control. The "Must Have" can also be considered an acronym for the Minimum Usable Subset and represents the elements that are the top priority and must be implemented to ensure compliance and the fundamental protection of systems and data.

Should Have: These are important, though not absolutely essential, features that are highly beneficial to the project but not mandatory for its initial launch. Their absence may cause some concern, but they would not cause the project to fail. These tasks can be added in future iterations if time or resource limitations exist. These are high priority but not critical items, which, while not strictly required for the project or policy to function, greatly enhance its value. For example, advanced logging and monitoring systems, though not always critical for smaller operations, significantly boost threat detection and response capabilities and should be implemented when possible.

Could Have: These are desirable features but less critical compared to "Must Have" and "Should Have" items. They are included if there is sufficient time and resources after more important tasks have been prioritized. These elements are often nice-to-haves that improve the user experience or system functionality but are not essential. In the context of cloud security, the "Could Have" category might include optional automation tools or third-party integrations that streamline processes but are not required to meet minimum security or compliance requirements.

Won't Have: This category refers to features or requirements that are deliberately excluded from the current scope, though they may be considered for future phases. These items help clarify expectations

and manage the scope effectively. These are lower-priority features that won't be implemented in the current project or policy version but may be revisited later. For example, an organization might decide to delay the use of specialized encryption techniques or niche cloud services until their infrastructure becomes more complex. [66,67]
A summary of MoSCoW Technique as presented in Purple Griffon, is represented below.[67]

Image 6.1: MoSCoW Technique [67]

Key Benefits of Using MoSCoW

Resource Allocation: The MoSCoW method ensures that time, budget, and personnel are allocated to the most critical security controls, ensuring the best return on investment for security efforts.

Clear Prioritization: By distinguishing between essential and non-essential elements, organizations can systematically roll out security controls while avoiding unnecessary delays.

Scalability: The framework allows businesses to tailor their security policies according to current needs while remaining flexible enough to adapt to future changes. [67, 68]

6.3 Policy

In this section, a framework has been created based on ISO 27002:2022 and AWS Best security practices. This framework can be used by organizations that have or wish to create infrastructure in the AWS cloud environment. Organizations can modify this depending on the infrastructure size and business needs.
First some information regarding the policy should be provided. Starting with

- Issue Date: The date that the policy is crafted
- Review Date: The date of the review
- Reviewers: Information: Usually name and surname,
- Document Owner: For instance, the head of IT Department or CISO
- Version: After every review, the version number, date, and description should be noted.

Table 6.1: Policy Information

Issue Date	dd/mm/yyyy
Next Review Date	MM YYYY
Reviewed by	Surname, Name
Document Owner	Surname, Name

Table 6.2: Version History

Version	Date	Modification Description

6.3.1 Introduction

This policy is designed to build a robust security framework that aligns with the controls and principles outlined in ISO 27002:2022, as well as AWS best security practices and CIS Amazon Benchmarks, to protect the organization's cloud infrastructure in accordance with the highest standards of cloud security. Its goal is to provide clear, actionable guidance for the management and protection of the organization’s information assets. By enforcing robust access control, data protection strategies,

incident response mechanisms, and continuous monitoring, this policy seeks to minimize risks, comply with regulatory obligations, and promote a culture of security awareness throughout the organization. This document serves as a foundational resource for all personnel, clarifying their responsibilities in safeguarding the organization's digital environment. Additionally, it is intended to be a dynamic document, regularly updated to address new threats and evolving technologies. By following the outlined protocols, the organization will enhance its ability to resist cyber threats and ensure the confidentiality, integrity, and availability of critical information.

6.3.2 Scope

This policy applies to all information assets, cloud infrastructure, and personnel within the organization, including employees, contractors, vendors, and any third parties with access to organizational systems or data. It covers all systems, applications, networks, devices, and cloud services, particularly those hosted on Amazon Web Services (AWS).

6.3.3 Glossary

AWS Amazon Web Services

IAM Identity and Access Management

MFA Multi-factor Authentication

AMI Amazon Machine Image

KMS Key Management Service

DAX DynamoDb Accelerator

EBS Elastic Block Service

EC2 Elastic Compute Cloud

EFS Elastic File System

RDS Relational Database Service

S3 Simple Storage Service

DLP Data Loss Prevention

SSL Secure Sockets Layer

ACL Access Control List

SQS Simple Queue Service

EDR Elastic Disaster Recovery

RTO Recovery Time Objectives

RPO Recovery Point Objectives

DNS Domain Name System

Chapter 6

VPC Virtual Private Cloud

SSH Secure Shell

RDP Remote Desktop Protocol

API Application Programming Interface

CMK Customer Master Key

NACL Network Access Control List

SNS Simple Notification Service

VPN Virtual Private Network

6.3.4 Policy Statements

6.3.4.1 Access Control and Management

[1] Access to information and related resources should be only allowed to individuals who are authorized, based on their roles and responsibilities within the organization.

[2] Privileged access should only be given to authorized users, software, or services that need such privileges to fulfill their duties. Permissions must be defined with the least privilege principle, ensuring users or roles only have the necessary access to perform their tasks.

[3] AWS IAM policies must not grant full administrative privileges to any users or roles. Instead, permissions should be clearly defined to ensure access is limited to necessary actions, following the least privilege principle.

[4] Multi-Factor Authentication (MFA) should be required for all IAM users with console access.

[5] Root users should have hardware-based MFA enabled.

[6] Root account should be prohibited from usage.

[7] Password policies must enforce strong password requirements, including a specific length, combination of uppercase and lowercase letters, numbers, and special characters, along with regular password updates.

[8] IAM policies should not be directly linked to individual IAM users. Instead, users should be assigned roles with predefined policies that correspond to their job functions to ensure a secure and scalable access structure.

[9] IAM access keys should be rotated every 90 days or less. Any unused or outdated access keys should be promptly disabled and removed.

[10] AWS root users should not have access keys. Root account access should only occur through strong authentication methods, and all actions taken by the root user should be limited and logged.

[11] Security questions should be set up in the AWS account to enhance the security of authentication procedures. [43, 50, 69, 70]

6.3.4.2 Data Security

[1] A consistent and standardized naming convention must be applied to all organizational AmazonMachine Images (AMIs) for uniformity and ease of identification. This convention should include key details such as creation date, operating system, description and version number to facilitate efficient management across different environments.

[2] All AMIs must be encrypted to ensure that the confidentiality and integrity of the data they contain are protected.

[3] Only AMIs that have undergone thorough review and approval by the organization's security team should be used in production and development environments. This process must include evaluations of security and performance to prevent the deployment of unverified or unauthorized AMIs.

[4] AMIs currently in use must be regularly updated and should not exceed 90 days in age. Older AMIs should either be updated to include the latest security patches or retired to maintain security standards.

[5] AMIs should not be made publicly available without explicit approval from the security team and relevant business stakeholders. Limiting public access to AMIs reduces the risk of exposing sensitive configurations and ensures better security controls.

[6] Data stored in Amazon Aurora databases must be encrypted to ensure the protection of sensitive information and compliance with internal security protocols and regulations.

[7] Data transmitted between Amazon Aurora databases and applications must be encrypted using TLS/SSL to ensure the integrity and confidentiality of information during transmission.

[8] Amazon DynamoDB Accelerator (DAX) clusters must use encryption at rest to safeguard cached data from unauthorized access and ensure alignment with data protection policies.

[9] All DynamoDB tables must have deletion protection enabled to prevent accidental or unauthorized removal of critical data.

[10] Data moving to and from DynamoDB Accelerator (DAX) clusters must be encrypted in transit using TLS/SSL to prevent unauthorized interception or tampering.

[11] Encryption at rest is mandatory for all data stored in DynamoDB tables to protect sensitive information and meet established security standards.

[12] Encryption must also be applied to all data transmitted between DynamoDB and its clients to maintain confidentiality and guard against potential breaches.

[13] Public access to EBS snapshots must be disabled to prevent unauthorized access to the sensitive information they contain.

[14] Default encryption should be enabled for all new EBS volumes to ensure that they are automatically encrypted without requiring manual intervention.

[15] Unused EBS volumes should be identified and removed to avoid unnecessary costs and minimize potential security vulnerabilities.

[16] EC2 instances that have been stopped for more than 90 days must be reviewed and, if no longer needed, removed to optimize resource management.

[17] All EBS volumes should be configured for automatic deletion when the associated EC2 instance is terminated unless specifically required otherwise.

[18] Sensitive information, such as credentials or secrets, must not be stored in EC2 User Data to prevent inadvertent exposure or misuse.

[19] All file data stored in Amazon Elastic File System (EFS) must be encrypted at rest using AWS KMS.

[20] All Kinesis streams must be encrypted at rest using AWS KMS to ensure the confidentiality and integrity of the streaming data.

[21] All Amazon RDS database instances must have encryption enabled to safeguard the stored data and meet security requirements.

[22] Encryption must also be applied to snapshots of Amazon RDS clusters and databases to protect the confidentiality of backup data.

[23] Deletion protection must be enabled for all RDS clusters to prevent the accidental or unauthorized removal of critical databases.

[24] Similarly, deletion protection should be enabled for all RDS DB instances to ensure the security of production environments.

[25] Sensitive information must be masked or anonymized to reduce the risk of exposure and ensure compliance with relevant legal, regulatory, and contractual requirements.

[26] Systems must be in place to detect and prevent unauthorized disclosure or extraction of sensitive information. Data Loss Prevention (DLP) tools should be implemented to monitor, control, and restrict data transfers via network channels or external devices.

[27] All information must be classified based on its importance, sensitivity, and potential impact. Appropriate security controls must be applied based on the classification to maintain confidentiality, integrity, and availability. Labels should assist in automating the management of information and must be visible to authorized personnel.

[28] Information being transferred within the organization or to external parties must be secured using encryption and secure transfer protocols to protect data integrity and confidentiality during transmission.

[29] Cryptographic techniques must be used to secure sensitive data, ensuring compliance with business needs, legal, regulatory, and contractual obligations.

[30] Public access to all S3 general-purpose buckets must be blocked by default to prevent unauthorized data exposure. Exceptions must be approved and documented.

[31] All access to S3 general-purpose buckets must be conducted over SSL to ensure secure data transmission and prevent interception.

[32] Access to S3 general-purpose buckets must be limited to authorized AWS accounts, with any cross-account access requiring justification and approval.

[33] Server access logging must be enabled for all general-purpose S3 buckets to track access and detect suspicious activities, with logs retained as per the organization's policy.

[34] Access to S3 general-purpose buckets must be managed through IAM policies, rather than ACLs, to ensure robust access control management.

[35] Lifecycle policies must be implemented for all S3 general-purpose buckets to manage data retention, archiving, and deletion in accordance with organizational and regulatory requirements.

[36] All Amazon SQS queues must be encrypted at rest using AWS KMS to protect the confidentiality of messages stored in the queue. [43, 50, 69, 70]

6.3.4.3 Data Backup and Recovery

[1] Critical data and system configurations must undergo regular backups to ensure recovery in the event of data loss, corruption, or system failure. The backup strategy should ensure all vital information is safeguarded in line with business and regulatory obligations.

[2] Backups must be encrypted using AWS Key Management Service (KMS) or equivalent encryption methods.

[3] AWS Backup plans must include Amazon Elastic File System (EFS) volumes to ensure automated, consistent backups for reliable data recovery.

[4] Amazon EFS file systems should have automatic backup features enabled to generate regular snapshots for recovery in the event of data loss or corruption.

[5] Automated backups must be enabled for Amazon Aurora, RDS, and DynamoDB, with retention policies applied to allow for timely data recovery. These retention periods should align with both organizational needs and legal requirements.

[6] Elastic Disaster Recovery (EDR) should be set up for all critical systems to ensure swift recovery in case of a disaster or major outage.

[7] AWS Disaster Recovery configurations must be optimized to meet the Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) specified in the organization's business continuity plan.

[8] Endpoint Detection and Response (EDR) systems must be thoroughly tested to confirm their effectiveness during disaster recovery scenarios, identifying potential issues during failover processes.

[9] Proper Identity and Access Management (IAM) configurations must be implemented for AWS Elastic Disaster Recovery to restrict disaster recovery operations to authorized personnel only.

[10] The AWS Replication Agent must be correctly installed and configured on all critical servers to ensure reliable data replication through AWS Elastic Disaster Recovery.

[11] Launch settings in Elastic Disaster Recovery should reflect production environment configurations to guarantee proper provisioning during system recovery.

[12] Regular recovery drills must be conducted to assess the preparedness of the AWS Disaster Recovery solution and identify any potential shortcomings in the recovery process.

[13] Continuous monitoring of disaster recovery activities is required to ensure ongoing replication and the readiness of recovery systems.

[14] Routine disaster recovery failover tests must be carried out to verify the systems' and team's readiness for a full failover situation.

[15] AWS CloudWatch Metrics must be set up and continuously monitored to assess the health, performance, and effectiveness of Elastic Disaster Recovery operations.

[16] Regular testing and validation of Elastic Disaster Recovery (EDR) must be performed to confirm the reliability and overall performance of the disaster recovery solution. [43, 50, 69, 70, 71]

6.3.4.4 Network Security

[1] The network should be segmented into distinct zones, and traffic between these zones must be filtered and monitored based on business needs, ensuring secure boundaries and minimizing the risk of unauthorized access.

[2] AWS Network Firewalls must have logging enabled to monitor all traffic and be configured with deletion protection to prevent accidental or malicious removal.

[3] Each AWS Network Firewall must have at least one rule group in place, with the default actions set to either "drop" or "forward" for complete or fragmented packets, ensuring strict traffic management.

[4] Public hosted zones in AWS Route 53 must have DNS query logging enabled to maintain visibility into all DNS activities and identify potential security risks.

[5] Stateless Network Firewall rule groups must always contain at least one rule to prevent security gaps.

[6] The default VPC should not be used for production workloads to maintain a secure network environment.

[7] VPC Flow Logs must be enabled across all applicable regions to capture and monitor network traffic for security and compliance purposes.

[8] The default security group must be configured to block all inbound and outbound traffic by default, ensuring secure baseline settings.

[9] Inbound traffic from 0.0.0.0/0 on port 22 (SSH) and port 3389 (RDP) should be strictly prohibited unless explicitly required and documented for specific use cases.

[10] EFS mount targets must not be placed in public subnets to prevent exposure of critical file systems to the internet. [43, 50, 69, 70]

6.3.4.5 Incident Detection and Response

[1] A formalized incident response plan must be in place to promptly detect, report, and respond to security incidents, including clear communication protocols for stakeholders during security events.

[2] All evidence gathered during security incidents must be preserved securely to support potential legal or disciplinary actions.

[3] Systems must include disaster recovery capabilities, such as regular backups and failover solutions, to ensure uninterrupted service during disruptions or breaches. [43, 50, 51]

6.3.4.6 Monitoring and Logging

[1] Privileged access to systems must be rigorously controlled, with all actions being logged via AWS CloudTrail, and logs regularly reviewed for unusual activities.

[2] AWS CloudTrail must be activated in all regions, with logs validated for integrity and integrated with AWS CloudWatch for real-time monitoring and alerts.

[3] All logs, including CloudTrail logs stored in S3, must be encrypted with AWS KMS to protect data integrity and ensure compliance with security policies.

[4] Automated monitoring must be deployed to detect abnormal behaviors, such as unauthorized API calls or IAM policy changes, with real-time alarms configured for prompt response.

[5] System and network events must be logged comprehensively to provide audit trails for investigations and ensure the integrity and security of log data.

[6] Monitoring tools must identify unusual behavior, particularly in privileged account activity and unauthorized access attempts.

[7] Production EC2 instances must have detailed monitoring enabled through AWS CloudWatch, with alarms configured for potential performance issues or security threats.

[8] Database auditing must be activated to track access and query activities, ensuring that sensitive data access is monitored and protected.

[9] CloudTrail logs in S3 must be encrypted at rest using KMS customer master keys (CMKs), with logging enabled to track and restrict unauthorized access to these logs.

[10] Customer-generated encryption keys must be rotated regularly to enhance security, and alarms must be set to detect any disabling or deletion of keys.

[11] A log metric filter and alarm must be in place for any usage of the root account. Root account access should be highly restricted and only used in emergency scenarios.

[12] A log metric filter and alarm must be in place for any AWS Management Console sign-ins that occur without Multi-Factor Authentication (MFA), ensuring that accounts are protected with an additional security layer.

[13] Alarms must be set to monitor root account usage, which should be strictly limited to emergency scenarios only.

[14] Any AWS Management Console logins that do not use Multi-Factor Authentication (MFA) must trigger an alert, reinforcing the use of additional security measures.

[15] CloudTrail configuration changes must be logged and monitored to prevent unauthorized modifications to the monitoring setup.

[16] AWS Config must be active in all regions to continuously monitor resource configurations, with alarms triggered by unauthorized changes.

[17] Any changes to security group configurations must be logged, particularly those that allow access from unrestricted IP addresses.

[18] Network-related changes, such as alterations to NACLs, gateways, or route tables, must be logged and monitored to detect unauthorized modifications.

[19] VPC alterations, including the creation, deletion, or modification of configurations, must be logged and reviewed regularly to prevent unauthorized changes.

[20] Ensure that key individuals and systems are subscribed to receive SNS alerts for critical security and system events.

[21] Accurate security contact information must be registered with AWS to receive critical security notifications and updates. [43, 50, 69, 70]

6.3.4.7 Asset Management

[1] All information and associated assets must be clearly identified and assigned ownership to ensure that they are used responsibly and adequately protected.

[2] Proper procedures must be followed to safeguard assets when employees leave the company or contracts are terminated, ensuring no unauthorized access to sensitive information. [43, 50, 69, 70]

6.3.4.8 Suppliers – Third-party Partners

[1] Suppliers must comply with the organization’s security requirements, and regular reviews should be conducted to verify that security controls are maintained throughout the relationship.

[2] Information security and service delivery requirements must be aligned with supplier contracts, ensuring consistent protection of sensitive information during service delivery. [43, 50, 69, 70]

6.3.4. 9 Compliance and Audit

[1] Regular audits must be carried out to ensure compliance with all legal, regulatory, and contractual obligations, especially those related to intellectual property, personal data protection (PII), and information security policies.

[2] Internal audits must be performed to verify that the organization’s information security controls and processes align with established policies, procedures, and standards. [43, 50, 69, 70]

6.3.4.10 Personnel Policy

[1] All personnel must meet the necessary qualifications and suitability criteria for their roles. Periodic reassessments should be conducted to ensure that they continue to meet the established standards.

[2] Employees must be informed about their responsibilities concerning information security and the repercussions of non-compliance with security policies. Clear instructions on how to report information security incidents must be communicated to all staff members.

[3] When an employee's role changes or their contract ends, access to company systems, data, and physical spaces must be revoked without delay to safeguard organizational interests. All company assets, such as devices, access cards, and confidential materials, must be returned.

[4] Any information accessed by employees or third parties must be treated as confidential during and after their relationship with the organization. Strict access controls must be implemented to ensure that only authorized individuals can view or handle sensitive information.

[5] Employees working remotely must adhere to robust security protocols, such as using secure networks (e.g., VPNs), encrypted communications, and ensuring their devices comply with security policies to protect corporate data.

[6] Employees are required to promptly report any suspected or confirmed information security incidents. The organization must establish consistent procedures for efficiently reporting, documenting, and resolving such incidents.

[7] Sensitive information and assets must be managed with caution, particularly within restricted areas. Only authorized personnel should be granted access to these areas, with adequate security measures in place to prevent unauthorized entry or damage.

[8] Personnel must ensure that confidential materials, whether on desks, screens, or other visible surfaces, are shielded from unauthorized access both during and outside working hours. This includes locking screens, securing sensitive documents, and adhering to a clean desk policy.

6.3.5 ISO References

- 5.9 Inventory of information and other associated assets
- 5.10 Acceptable use of information and other associated assets
- 5.11 Return of assets
- 5.12 Classification of information
- 5.13 Labeling of information
- 5.14 Information transfer
- 5.15 Access control
- 5.19 Information security in supplier relationships
- 5.20 Addressing information security within supplier agreements
- 5.21 Managing information security in the ICT supply chain
- 5.22 Monitoring, review and change management of supplier services
- 5.24 Information security incident management planning and preparation
- 5.26 Response to information security incidents
- 5.27 Learning from information security incidents
- 5.28 Collection of evidence
- 5.29 Information security during disruption
- 5.31 Legal, statutory, regulatory and contractual requirements
- 5.32 Intellectual property rights
- 5.33 Protection of records
- 5.34 Privacy and protection of PII
- 5.36 Compliance with policies, rules and standards for information security
- 6.1 Screening
- 6.2 Terms and conditions of employment
- 6.3 Information security awareness, education and training
- 6.4 Disciplinary process
- 6.5 Responsibilities after termination or change of employment
- 6.6 Confidentiality or non-disclosure agreements

- 6.7 Remote working
- 6.8 Information security event reporting
- 7.6 Working in secure areas
- 7.7 Clear desk and clear screen
- 8.2 Privileged access rights
- 8.5 Secure authentication
- 8.11 Data masking
- 8.12 Data leakage prevention
- 8.13 Information backup
- 8.14 Redundancy of information processing facilities
- 8.15 Logging
- 8.16 Monitoring activities
- 8.17 Clock synchronization
- 8.20 Network security
- 8.21 Security of network services
- 8.22 Segregation of networks
- 8.23 Web filtering
- 8.24 Use of cryptography

6.3.6 AWS References

- AWS Control “IAM.1”
- AWS Control “IAM.2”
- AWS Control “IAM.3”
- AWS Control “IAM.4”
- AWS Control “IAM.5”
- AWS Control “IAM.6”
- AWS Control “IAM.7”
- AWS Control “IAM.8”
- AWS Control “IAM.21”
- AWS Control “DynamoDB.3”
- AWS Control “DynamoDB.6”
- AWS Control “DynamoDB.7”
- AWS Control “EC2.1"
- AWS Control “EC2.3"
- AWS Control “EC2.7"
- AWS Control “EFS.1"
- AWS Control “EFS.2”
- AWS Control “EFS.6”
- AWS Control “EFS.7”
- AWS Control “Kinesis.1"
- AWS Control “RDS.3"
- AWS Control “RDS.4"
- AWS Control “RDS.7"
- AWS Control “RDS.8"
- AWS Control “RDS.27"

- AWS Control “S3.1”
- AWS Control “S3.2”
- AWS Control “S3.3”
- AWS Control “S3.5”
- AWS Control “S3.6”
- AWS Control “S3.8”
- AWS Control “S3.9”
- AWS Control “S3.12”
- AWS Control “S3.13”
- AWS Control “S3.19”
- AWS Control “SQS.1"
- AWS Control “Backup.1”
- AWS Control “NetworkFirewall.2”
- AWS Control “NetworkFirewall.3”
- AWS Control “NetworkFirewall.4”
- AWS Control “NetworkFirewall.5”
- AWS Control “NetworkFirewall.6”
- AWS Control “NetworkFirewall.9”
- AWS Control “Route53.2”

6.3.7 CIS Amazon Web Services Foundations References

- IAM 1.1
- IAM 1.14
- Networking 4.1
- Networking 4.2
- Networking 4.3
- Networking 4.4
- Logging 2.1
- Logging 2.2
- Logging 2.3
- Logging 2.4
- Logging 2.5
- Logging 2.6
- Logging 2.7
- Logging 2.8
- Monitoring 3.1
- Monitoring 3.2
- Monitoring 3.3
- Monitoring 3.4
- Monitoring 3.5
- Monitoring 3.6
- Monitoring 3.7
- Monitoring 3.8
- Monitoring 3.9

- Monitoring 3.10
- Monitoring 3.11
- Monitoring 3.12
- Monitoring 3.13
- Monitoring 3.14
- Monitoring 3.15
- Monitoring 3.16

6.3.8 CIS Compute Services Benchmark References

- AMI 2.1.1
- AMI 2.1.2
- AMI 2.1.3
- AMI 2.1.4
- AMI 2.1.5
- EBS 2.2.1
- EBS 2.2.2
- EBS 2.2.3
- EBS 2.2.4
- EBS 2.6
- EBS 2.10
- EBS 2.11
- EBS 2.12
- EBS 2.13

6.3.9 CIS Database Services Benchmark References

- Aurora 2.3
- Aurora 2.4
- Aurora 2.6
- Aurora 2.10
- DynamoDB 4.3
- DynamoDB 4.4
- DynamoDB 4.7
- RDS 3.6
- RDS 3.9
- RDS 3.10

6.3.10 CIS AWS Storage Services Benchmark References

- EDR 6.1
- EDR 6.2
- EDR 6.3
- EDR 6.4
- EDR 6.5
- EDR 6.6
- EDR 6.7
- EDR 6.8

- EDR 6.9
- EDR 6.10
- EDR 6.11
- EDR 6.12
- EDR 6.13
- EBS 2.2
- EBS 2.12

6.4 Applying MoSCoW Prioritization

Considering the policy framework outlined, a MoSCoW method can also be applied. This approach helps prioritize policy elements into four categories based on the organization's size and needs:

Must Have:

- Access Control: Clearly defined user roles, and restricted privileged access are obligatory..
- Data Protection: Encryption, regular backups, and proper data classification across the organization must be enforced in order to safeguard sensitive information.
- Incident Response Plan: A structured approach for handling security incidents is obligatory to be established for efficient and timely mitigation.
- Compliance: Continuous compliance with legal and regulatory requirements.

Should Have:

- Network Security: Implement secure network configurations, with some flexibility for smaller organizations based on their capacity.
- Asset Management: Strongly enforce the tracking and control of hardware and software assets to minimize risks.
- Training and Awareness: Training should be mandatory for all employees, with adjustments for smaller organizations if necessary.

Could Have:

- Cloud Best Practices: While cloud-specific security practices (like those for AWS) should be considered, smaller organizations may scale them based on their level of cloud usage.
- Advanced Monitoring and Automation: Tools like SIEM systems could be valuable, but they may not be immediately essential for small to medium-sized businesses.

Won’t Have (for now):

- Highly Customized Controls: Developing custom security tools or frameworks may not be a priority.
- Full Automation: Smaller businesses may not require fully automated security incident responses or vulnerability management processes.

6.5 Epilogue

As the development of a robust information security policy framework for small to medium-sized organizations has been completed, it is crucial to highlight the dynamic nature of security management. Implementing and maintaining the effectiveness of a comprehensive policy framework requires continuous effort and adaptability. Also, requires regular reviews in order to always be updated and effective. Finally, clear and documented operating procedures are essential for the consistent application of security policies. These procedures should be detailed and accessible to all relevant personnel, providing a solid foundation for the implementation and enforcement of security measures.

Chapter 6

Chapter 7: Future Steps and Next Goals

7.1 Conclusion

In this thesis, we studied how cyber threats have evolved and how they can affect organizations. We studied the importance of security frameworks' existence by examining the most widely known protocols like ISO and highlighting their key aspects and benefits. Then, we described a well-structured framework that can lay the groundwork for robust information security. By implementing this policy, organizations that already have or planning to migrate their infrastructure to AWS can manage and safeguard their data and assets in general.

7.2 Future Steps

As information security continues to evolve, the focus will shift towards updating and extending the policy framework developed for AWS to other major cloud providers, specifically Microsoft Azure and Google Cloud Platform (GCP) to reflect their services and best practices. This expansion aims to ensure comprehensive security practices across a multi-cloud environment, addressing the unique challenges and requirements posed by each platform.

7.3 Next Goals

The next goals will involve

- Developing Security Frameworks: Create tailored security policies for Azure and GCP that align with each platform’s unique features and compliance requirements.
- Ensuring Integration: Make sure these new frameworks integrate smoothly with the existing AWS policies for a unified security strategy across all cloud environments.
- Continuous Improvement: Regularly update the frameworks to address new risks, technologies, and compliance changes.
- Independent Review: Seek external audits to validate the effectiveness of the new frameworks and ensure they meet high security standards.
- Documentation and Training: Provide clear documentation and training for the new frameworks to ensure effective implementation and adherence.

These steps will enhance our multi-cloud security posture and ensure robust protection across all platforms.

Chapter 7

Chapter 8: References

[1] Y. Alghofaili, A. Albattah, N. Alrajeh, M. A. Rassam, and B. A. S. Al-Rimy, “Secure cloud infrastructure: A survey on issues, current solutions, and open challenges”

[2] Microsoft, What is Cloud Computing: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-computing

[3] AWS, AWS Cloud Products: https://aws.amazon.com/products/?aws-products-all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-order=asc&awsf.re%3AInvent=*all&awsf.Free%20Tier%20Type=*all&awsf.tech-category=*all

[4] P. M. Mell and T. Grance, “The NIST definition of cloud computing,” Gaithersburg, MD, 2011. doi: 10.6028/NIST.SP.800-145.

[5] National Security Agency | Cybersecurity Information “Mitigating Cloud Vulnerabilities”

[6] Accenture, State of Cybersecurity Resilience 2023: https://www.accenture.com/content/dam/accenture/final/accenture-com/document/Accenture-State-Cybersecurity.pdf#zoom=40

[7] Checkpoint: Top Cloud Security Issues, Threats and Concerns: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/

[8] Sonrai Security, Tally Shea:IAM risks and how to mitigate them: https://sonraisecurity.com/blog/9-common-iam-risks-how-to-mitigate-them/

[9] MightyID, Exploring Common Identity and Access Management Risks: https://www.mightyid.com/articles/common-identity-and-access-management-risks

[10] AWS, AWS best practices ddos resiliency: https://docs.aws.amazon.com/whitepapers/latest/aws-best-practices-ddos-resiliency/aws-best-practices-ddos-resiliency.html

[11] NIST Special Publication, “Security and Privacy Controls for Information Systems and Organizations,” Sep. 2020.

[12] Gary Smith, 75+ Surprising Cloud Security Statistics You Should Know in 2024: https://www.stationx.net/cloud-security-statistics/

[13] Fortinet, Man-in-the-Middle Attack: Types and Examples: https://www.fortinet.com/resources/cyberglossary/man-in-the-middle-attack

[14] OWASP, SQL Injection: https://owasp.org/www-community/attacks/SQL_Injection

[15] IBM, Cost of a Data Breach report in 2024: https://www.ibm.com/reports/data-breach

[16] OWASP, Cloud-Native Application Security Top 10: https://owasp.org/www-project-cloud-native-application-security-top-10/

[17] Aquasec, Amit Seps, Top 10 Cloud Attacks and What You Can Do About Them: https://www.aquasec.com/cloud-native-academy/cloud-attacks/cloud-attacks/

[18] Spiceworks, Ramya Mohanakrishnan, What Is Incident Response? Definition, Process, Lifecycle, and Planning Best Practices: https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-incident-response/

[19] NIST, Paul Cichonski, Tom Millar, TimGrance, Karen Scarfone, Computer Security Incident Handling Guide
[20] Tri Widianti, Anggini Dinaseviani, Meilinda Ayundyahrini, Sik Sumaedi and Tri Rakhmawati, Nidya Judhi Astrini and I Gede Mahatma Yuda Bakti, Sih Damayanti, Medi Yarmen and Rahmi Kartika Jati, Aris Yaman, Marlina Pandin, Mauludin Hidayat, Igif Gimin Prihanto, Hendy Gunawan and Mahmudi Mahmudi, "Business continuity management: trends, structures and future issues" Jun 2024 DOI 10.1108/BPMJ-01-2024-0046.
[21] IBM, What is Threat Intelligence: https://www.ibm.com/topics/threat-intelligence
[22] Stavridis Kyriakos, "Ευφυές σύστημα διαχείρισης πληροφοριών και περιστατικών ασφαλείας (SIEM)"
[23] Spiceworks, Remya Mohanan, What Is Security Information and Event Management (SIEM)? Definition, Architecture, Operational Process, and Best Practices: https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-siem/
[24] Microsoft, What is endpoint detection and response (EDR)?: https://www.microsoft.com/en-us/security/business/security-101/what-is-edr-endpoint-detection-response
[25] OpenEDR, What is EDR?: https://www.openedr.com/blog/what-is-edr/
[26] Tunboson Oyewale Oladoyinbo, Olubukola Omolara Adebiyi, Jennifer Chinelo Ugonnia, Oluwaseun Oladeji Olaniyi, Olalekan J. Okunleye,Evaluating and Establishing Baseline Security Requirements in Cloud Computing: An Enterprise Risk Management Approach
[27] CloudFlare, What is Zero Trust security?: https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/
[28] Crowdstrike, CLOUD SECURITY FRAMEWORKS: HOW TO CHOOSE THE RIGHT ONE FOR YOUR BUSINESS: https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-security-frameworks/
[29] Wikipedia, Center of Internet Security: https://en.wikipedia.org/wiki/Center_for_Internet_Security
[30] Center of Internet Security: https://www.cisecurity.org/about-us
[31] CIS,CIS Critical Security Controls Version 7 – What's Old, What's New: https://www.cisecurity.org/insights/blog/cis-controls-version-7-whats-old-whats-new
[32] CIS, Getting to Know the CIS Benchmarks: https://www.cisecurity.org/insights/blog/getting-to-know-the-cis-benchmarks
[33] Cloud Security Alliance, Security, Trust, Assurance and Risk(STAR): https://cloudsecurityalliance.org/star
[34] Cloud Security Alliance, Cloud Controls Matrix: https://cloudsecurityalliance.org/research/cloud-controls-matrix
[35] Cloud Security Alliance, STAR-Level-and-Scheme-Requirements: https://cloudsecurityalliance.org/artifacts/star-level-and-scheme-requirements
[36] Wikipedia, International Organization for Standardization: https://en.wikipedia.org/wiki/International_Organization_for_Standardization
[37] ISO, Popular standards and other ISO deliverables: https://www.iso.org/popular-standards.html
[38] ISO, ISO/IEC 27001: https://www.iso.org/standard/27001
[39] Wikipedia,ISO/IEC 27017: https://en.wikipedia.org/wiki/ISO/IEC_27017
[40] ISO, ISO/IEC 27017: https://www.iso.org/standard/43757.html

[41] Wikipedia,ISO/IEC 27002: https://en.wikipedia.org/wiki/ISO/IEC_27002
[42] Tuvsud, WHAT IS ISO/IEC 27017 AND WHO DOES IT APPLY TO?: https://www.tuvsud.com/en-in/services/auditing-and-system-certification/iso-iec-27017-security-control-for-cloud-services
[43] ISO, ISO/IEC 27002: https://www.iso.org/standard/75652.html
[44] Sprinto, Meeba Gracy, What is ISO 27002 Compliance and How to Implement it?: https://sprinto.com/blog/iso-27002-compliance/#Benefits_of_implementing_ISOIEC_27002
[45] Medium, Akitra, ISO 27002: Everything You Need To Know!: https://medium.com/@akitrablog/iso-27002-everything-you-need-to-know-a9fc84079ddc
[46] MITRE, ATT&CK, https://attack.mitre.org/resources/
[47] MITRE, Otis Alexander, Misha Belisle, Jacob Steele, MITRE ATT&CK® for Industrial Control Systems: Design and Philosophy.
[48] MITRE, ATT&CK, https://attack.mitre.org/
[49] MITRE, Getting Started with ATT&CK, Adam Pennington, Editor, Andy Applebaum, Katie Nickels, Tim Schulz, Blake Strom, John Wunder, https://www.mitre.org/sites/default/files/2021-11/getting-started-with-attack-october-2019.pdf
[50] AWS, AWS Foundational Security Best Practices (FSBP) standard: https://docs.aws.amazon.com/securityhub/latest/userguide/fsbp-standard.html
[51] AWS, AWS Security Reference Architecture: A guide to designing with AWS security services: https://aws.amazon.com/blogs/security/aws-security-reference-architecture-a-guide-to-designing-with-aws-security-services/
[52] Microsoft Security, Overview of Microsoft cloud security benchmark (v1): https://learn.microsoft.com/en-us/security/benchmark/azure/overview#controls
[53] Microsoft Security, Security Control: Network security: https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security
[54] Microsoft Security, Security Control: Identity Management: https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management
[55] Microsoft Security, Security Control: Privileged Access: https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access
[56] Microsoft Security, Security Control: Data Protection: https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection
[57] Microsoft Security, Security Control: Asset Management: https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-asset-management
[58] Microsoft Security, Security Control: Logging and Threat Detection: https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection
[59] Microsoft Security, Security Control: Incident Response: https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-incident-response
[60] Microsoft Security, Security Control: Posture and Vulnerability Management: https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management
[61] Microsoft Security, Security Control: Endpoint Security: https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-endpoint-security
[62] Microsoft Security, Security Control: Backup and Recovery: https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-backup-recovery
[63] Microsoft Security, Security Control: DevOps Security: https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-devops-security

Chapter 8

[64] Microsoft Security, Security Control: Governance and Strategy: https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy
[65] Microsoft, Overview of the Azure Security Benchmark Foundation blueprint sample: https://learn.microsoft.com/en-us/azure/governance/blueprints/samples/azure-security-benchmark-foundation/
[66] Wikipedia, MoSCoW Method: https://en.wikipedia.org/wiki/MoSCoW_method
[67] Purple Griffon, MoSCoW Technique: https://purplegriffon.com/blog/moscow-technique
[68] IDEASCALE, 6 Essential MoSCoW Analysis Advantages: https://ideascale.com/blog/moscow-analysis-advantages/
[69] AWS, AWS Well-Architected Framework (Security Pillar): https://docs.aws.amazon.com/pdfs/wellarchitected/latest/security-pillar/wellarchitected-security-pillar.pdf
[70] CIS, Amazon Web Services Benchmarks: https://www.cisecurity.org/benchmark/amazon_web_services
[71] AWS, AWS Well-Architected Framework (Reliability Pillar): https://docs.aws.amazon.com/pdfs/wellarchitected/latest/reliability-pillar/wellarchitected-reliability-pillar.pdf