Internship

MSc Research Project
MSc Cyberswecurity

Diwaker Prasad
Student ID: 23119411

School of Computing
National College of Ireland

Supervisor: Kamil Mahajan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Diwaker Prasad		
Student ID:	23119411		
Programme:	MSc Cybersecurity	**Year:**	2024
Module:	Internship		
Supervisor:	Kamil Mahajan		
Submission Due Date:	2nd September 2024		
Project Title:	Internship Part 2		
Word Count:	3500 **Page Count** 12		

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: ....

Date: ....

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

What settings specific to AWS configurations, services and best practices can be applied on AWS for ensuring the data security & compliance related to business expenses data storage by Bookkeeping organizations & processing in the territory of European & UK?

Diwaker Prasad
23119411
Programme Code – Research in Computing CA2

Abstract

With a growing number of digital threats in today's world, financial organizations need to have optimal data security, especially when it comes to compliance with such regulations as GDPR and CIS Controls. This paper explores implementation of AWS configurations in the case of financial services firm Capisso with specific focus on their data security and compliance requirements. The paper focuses on different AWS configurations relevant to GDPR articles and CIS Controls needed by the organization operating in the EU and UK dealing with financial information. The study results point at the importance of aligning the AWS services such as IAM, encryption solutions, and monitoring tools for addressing risks and compliance. Besides, it identifies gaps that may be addressed by Capisso to improve its security status and compliance strategy and serve as reference for other financial organizations effectively.

1 Introduction

It is observed that the financial organizations are fast embracing the cloud computing technology and this has brought about new challenges concerning the security of data and compliance to the regulations. Since most financial institutions have started outsourcing their management, processing, and storage of the financial data in cloud services, they are faced with numerous regulatory requirements especially in European and UK regions where GDPR data protection standards apply. Also, CIS Controls as the name suggests is another guide that a firm can use in an effort to protect its systems and data from possible cyber threats.

This study aims at exploring how Capisso, a financial bookkeeping services company, manages these problems with the help of configuring the Amazon Web Services (AWS). The first and foremost is to find out that configurations in AWS, guidelines under GDPR articles, and CIS Controls which are mandatory for Capisso to protect its financial information and to conform with regulations.

To the best of the author's knowledge, this study will enrich the existing research because it provides a comprehensive insight into clouds security in the context of the financial industry while stressing the importance of AWS configuration to meet the requirements of GDPR and CIS Controls. The research is structured as follows: Section 2 provides the background of related studies, Section 3 describes the research approach, Section 4 defines the design of the system, Section 5 explains the process of implementation, Section 6 discusses case studies and analyses the results obtained and Section 7 suggests the recommendations for the future work.

2 Related Work

The protection of data, and compliance within the financial industry is an important factor; this being when preserving data in the cloud cloud solution is rapidly gaining popularity. Many researchers have reviewed the issues and approaches on how to ensure the security of monetary data in the cloud and with reference to the GDPR regulation.

2.1 Cloud Security in Financial Organizations

It seems that cloud environments have revolutionalized how the financial institution handle their data, but not without some risks involved. Crowdstrike [1] identified several threats of cloud security in the financial organization they include data loss, sabotage insider threats and noncompliance with regulations. To minimize these risks, the authors stress on the need to have strong identity and access management controls, use of encryption techniques, and constant vigil. These security challenges are as follows; AWS offers Identity and Access Management (IAM) as well as Key Management Service (KMS) to meet them [2].

2.2 GDPR Compliance in the Cloud Environment

Specifically, GDPR has raised the bar as to what constitutes adequate data protection measures especially where the context is cloud computing. [3] discuss some of the challenges of achieving compliance with GDPR in cloud and discuss that there are primary responsibilities that data controllers must fulfil including the requirement to process data in an appropriate manner and to respect the rights of data subjects. Three key principles, namely encryption, access controls, and minimization of data handed out are some of the core tenets of GDPR compliance and all of which are integrated in the AWS configurations [3].

2.3 CIS Controls for Cloud Security

In particular the CIS Controls provide a good framework for implementing cloud security. CIS Controls have to be applied in the cloud environment only if it is safe and aligned with the organization’s security objectives. According to the study the best ways to increase compliance and improve security is by adopting service like AWS Config and GuardDuty [4].

This study indicates from the literature review that a major research study gap is that many studies have been conducted on cloud security and compliance, but few if any have specific to the needs of the financial sector in AWS configurations. In conducting this research, this paper seeks to address this gap to give a detailed understanding of how Capisso protects its financial information together with the adherence to GDPR and CIS Controls.

3 Research Methodology

This paper uses a single case research design with Capisso, a financial services firm based in Italy to discuss AWS configuration settings and compliance with GDPR and CIS Controls. The research entails interview, document review and an analysis of Capisso's AWS setting.

3.1 Data Collection

Data was collected from multiple sources, including:

- Document Analysis: Adherence to internal security polices as well as compliance reports and configurations documents regarding AWS usage.
- AWS Environment Examination: Direct assessment of selected AWS services that define the safe operation of Capisso's environment, such as IAM policies, encryption, and AWS CloudTrail.

3.2 Data Mapping

The gathered information was then compared to GDPR articles and CIS Controls to measure the effectiveness of the firm's security measures at Capisso. This mapping was to find out some unique settings in AWS which correspond to GDPR rules and CIS Control levels.

3.3 Analysis

Specifically, the evaluation was aimed at evaluating the compliance of the AWS configurations applied at Capisso with GDPR and CIS. The research compared IAM policies, the use of encryption, logging, and monitoring tools and determined the impact they have and where previously they lacked.

4 Design Specification

This somewhat concerns the cloud configuration, where design specification includes specified AWS configurations, GDPR Compliance, and CIS Controls to apply to secure financial data. The following are the key design elements:

4.1 Identity and Access Management (IAM)

IAM is important when it comes to regulating access to some of the highly sensitive data involving the company's financial processes. IAM also allows Capisso implement user's role-based access control as an efficient way of preventing unauthorized users to gain access to some sensitive resources. The use of Multi-Factor Authentication (MFA) is mandatory for any IAM users, in accordance to GDPR Article 32 that emphasizes on processing security and CIS Control 16 on Account Monitoring and Control [5].

4.2 Data Encryption

Data encryption is created by AWS Key Management service for data at rest and in transit data encryption also. This complies with GDPR Regulation 25 which deals with Data

Protection by Design and by Default and CIS Control 13 of Data Protection. Encryption is used to safeguard the privacy of such financial information especially in the event that the underlying storage is compromised [6], [7].

4.3 Monitoring and Logging

The login activity and all events in the AWS environment of Capisso is logged through AWS CloudTrail and GuardDuty respectively. This meets the GDPR's Article 30 (Records of Processing Activities) and CIS Control 6 (Maintenance, Monitoring, and Analysis of Audit Logs). The applicaiton of these tools guarantees constant surveillance and identification of possible security threats [8].

4.4 Incident Response

Capisso has also worked at establishing an incident response plan with the help of AWS Config as well as SNS for notifications. This plan fits GDPR standards namely Article 33 (Notification of a Personal Data Breach to the Supervisory Authority) under Data Protection Regulation as well as CIS Control 17 (Incident Response and Management). The particular about the security of data is that the incident response plan is tested now and then for the purposes of readiness [9] [10].

5 Implementation

This brought into emphasis the design of the solution where the proposed solution involved customizing AWS services to address the various findings from the GDPR requirements and CIS Controls highlighted above. The following steps were taken to implement the solution:

Table 1: AWS Configurations and GDPR Compliance at Capisso

Category	**GDPR Requirement**	**CIS Control**	**Level**	**AWS Configuration**	**Implemented by Capisso**
IAM	Access Control (Article 32)	MFA for Root Account	Level 1	MFA should be enabled for root account	Yes
	Data Confidentiality (Article 32)	MFA for All IAM Users	Level 1	MFA should be enabled for all IAM Users	Yes
	Third-Party Security (Article 28)	MFA for IAM Users	Level 1	MFA should be enforced for all users	Yes
Storage	Data Protection (Article 32)	Monitor S3 Bucket Policies	Level 1	Configure AWS Config rules to monitor S3 bucket policies	No
	Data Minimization (Article 5)	Role-Based Access Control	Level 1	Set up AWS Config to monitor CMK deletion	No
	Data Protection	AWS Shield	Level	Activate AWS	No

Category	**GDPR Requirement**	**CIS Control**	**Level**	**AWS Configuration**	**Implemented by Capisso**
	Against Destruction (Article 32)		2	Shield for DDoS protection	
	Data Confidentiality & Integrity (Article 32)	Encryption at Rest	Level 1	Enable encryption for S3, EBS, RDS, etc.	Yes
	Secure Data Storage (Article 32)	Proper Storage Configuration	Level 2	Implement secure S3 Bucket and EBS configurations	No
EC2	Data Confidentiality (Article 32)	Secure OS Configurations	Level 1	Harden OS Configurations for EC2 Instances	No
	Technical Measures for Security (Article 32)	Secure Network Configurations	Level 2	Configure Security Groups, NACLs, VPCs	Not Sure
RDS	Data Protection by Default (Article 25)	Encryption for RDS Instances	Level 1	Enable RDS encryption	Not Sure
EFS	Data Protection (Article 32)	Monitor S3 Bucket Policies	Level 1	Configure AWS Config to monitor S3 Bucket Policies	No
Logging	Data Breach Prevention (Article 33)	Log Access and Events	Level 1	Enable CloudTrail, CloudWatch Logs	Yes
	Security Measures Testing (Article 32)	Vulnerability Management	Level 1	Implement AWS Inspector	No
Monitoring	Security Incident Detection (Article 32)	Continuous Monitoring & Alerting	Level 1	Enable GuardDuty, CloudWatch Alarms	No
Networking	Data Transparency & Accountability (Article 12)	Restrict Remote Admin Port Access	Level 2	Configure Security Groups to limit access	No
	Secure Processing (Article 32)	Secure SSH Access	Level 2	Implement SSH key pairs, Security Groups	No
	Data Integrity & Confidentiality (Article 5)	Data Protection by Design	Level 2	Design secure architecture using best practices	No
	Data Minimization (Article 5)	Least Privilege Access	Level 1	Implement IAM Policies and Roles	Yes

Category	GDPR Requirement	CIS Control	Level	AWS Configuration	Implemented by Capisso
	Secure Data Destruction (Article 17)	Secure Deletion Policies	Level 2	Use AWS Key Management Service (KMS), secure wipe tools	No
General	Data Availability & Resilience (Article 32)	Regular Automated Backups	Level 1	Enable AWS Backup, S3 Versioning	No
	Data Lifecycle Management (Article 5)	Monitor CMK Deletion	Level 1	Use AWS Config to monitor CMK lifecycle	No
	Data Subject Rights (Article 15)	Secure Data Portals	Level 1	Implement secure data access portals	Not Sure
	Data Breach Notification (Article 34)	Incident Response Plan	Level 2	Develop and test an Incident Response Plan	No
	Data Security (Article 32)	Regular Penetration Testing	Level 2	Conduct regular penetration tests on AWS resources	No
	Data Confidentiality During Processing (Article 32)	Data Masking Techniques	Level 1	Implement data masking in RDS, Redshift, etc.	No
	Data Availability (Article 32)	Redundancy & Backups	Level 1	Use multi-AZ deployments, AWS Backup	Yes

6 Evaluation

The purpose of this section is to provide a comprehensive analysis of the results and main findings of the study as well as the implications of these finding both from academic and practitioner perspective are presented. Only the most relevant results that support your research question and objectives shall be presented. Provide an in-depth and rigorous analysis of the results. Statistical tools should be used to critically evaluate and assess the experimental research outputs and levels of significance [11].

6.1 Access Control (IAM)

This principle was put to a test by deploying IAM in order to confirm that the use of the least privilege was proper. The study findings were that all the users had the correct levels of permissions to the extent that they required for their tasks without seeking more than what was required from them. Multi Factor Authentication also known as MFA were implemented and the policy for enforcing MFA was successfully put to practice to ensure all users had MFA on their accounts. This setup can be used in compliance with GDPR Article 32 and CIS Control 16 [11] [10].

6.2 Data Encryption

Data encryption was assessed based on data that are stored and data that are transmitted across the different networks. It was observed that use of AWS KMS for encryption was successful in providing safety to financial data. End-to-end encryption of data was validated through tests indicating that all stored data was encrypted through customer-managed keys, along with data in transit, by TLS. These keep one’s information safe from unauthorized access,thus satisfying GDPR Article 25 and CIS Control 13 [12].

6.3 Monitoring and Logging

Two specific control techniques which were monitoring and logging were evaluated based on AWS CloudTrail logs as well as GuardDuty alerts. Further, from the evaluation, it was clear that the current setup involved detailed logging of all API calls and the related access events with no breaks in the logs. With this exposure, GuardDuty achieved the purpose of finding and reporting threat sources of its security team, including unauthorized access attempts. The guidelines provided in this monitoring framework will facilitate compliance with GDPR Article 30 and CIS Control 6 [13].

6.4 Incident Response

The identified Incident Response Plan consisted of assessment and examination through security security incidents. AWS Config rules can identify compliance violations and, therefore, identify deviations from security policies, while SNS immediately informed the security team. The response times were tolerable and it showed preparedness to deal with the real breaches. This is in line with the GDPR Article 33 and CIS Control 17 to enable Capisso have a quick response to breaching of data [6].

6.5 Compliance Mapping

To add more weight to the various configurations a cross check was done where the configured AWS settings were compared with the GDPR articles and the CIS Controls. The mapping confirmed that Capisso's AWS environment is aligned with the following compliance requirements [14], [15]:

GDPR Articles:

Article 25: Data protection by design and by default

The specific provisions of Article 30 of the GDPR are entitled Records of Processing Activities.

Article 32: Processing under the control of the Controller

Regulation (EU) 2016/679 of the European Parliament and of the Council > Chapter V > Article 33: Notification of a Personal Data Breach to the Supervisory Authority

CIS Controls:

7 Control: System Monitoring and Logging at Level 1

Control 13 Data Protection – at Level 1

Control 16: 'The second level of account monitoring and control".

Control 17: Incident Response and Management (Level 2) of the security control catalog is defined as the process through which information security personnel examine an event and its impact on an organization's systems and data and determine the appropriate course of action that will recover the affected assets to a predefined state while maintaining documented and approved guidelines as well as expertise.

The compliance mapping showed that identified configurations in AWS platform are enough to address GDPR and CIS requirements relevant to Capisso.

7 Discussion

According to the evaluation results this approach can be considered as sufficiently reliable and suitable for organizing AWS configurations needed to address the security and compliance requirements within the sphere of financial organization working within the EU and UK regulations. So, the IAM policies, the mechanisms of encryption, and the monitoring tools provided by Capisso match the requirements of GDPR and CIS Controls, thus allowing a company avoiding data breaches and meeting the requirements of the legislation.

Nevertheless, there were some suggestions for further development. For instance, although the current setup of monitoring is sufficient, having multiple levels of anomaly detection and incorporating machine learning-powered threats identification tools will be beneficial. Also, the incidents response plan can further be enhanced regarding more elaborate test cases that are needed for all possible types of security threats.

8 Conclusion and Future Work

Where AWS Configurations are crucial for financial organisations and how Capisso has been designed to meet GDPR and CIS Control compliance. The study has also exposed how IAM, KMS, CloudTrail and Amazon GuardDuty services help secure the financial data and meet regulatory requirements.

The results presented in this paper prove that Capisso's experience regarding cloud security is effective and compliant with GDPR and CIS regulations. With proper access rights, proper encryption and constant surveillance, Capisso has developed a secure cloud setting where financial data is shielded from outside interference and the firm's regulatory requirements are met.

However, the study also reveals the opportunities by which Capisso can build more security into its system. Further research could focus on the implementation of new improved threat detection systems for instance, the use of machine learning in modeling anomaly detection systems for improvement of the monitoring and handling of security incidents. Also, the involvement of a broader set of scenarios in the development of the incident response plan would suggest that the organization is better prepared for any number of different security incidents from actual, to potential to suspected.

The study helps enriching the existing body of knowledge regarding cloud security practices in the financial sector and provides useful recommendations to other organizations in making sense of the highly complex issues of data security and compliance in the era of cloud computing.

References

[1] "12 Cloud Security Issues: Risks, Threats & Challenges," crowdstrike.com. Accessed: Sep. 02, 2024. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-security-risks-threats-challenges/

[2] I. Khalil, A. Khreishah, and M. Azeem, "Cloud Computing Security: A Survey," *Computers*, vol. 3, pp. 1–35, Mar. 2014, doi: 10.3390/computers3010001.

[3] S. Kanungo, "Data Privacy and Compliance Issues in Cloud Computing: Legal and Regulatory Perspectives," *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 21s, Art. no. 21s, Apr. 2024.

[4] "What is CIS Benchmarks? - CIS Benchmarks Explained - AWS," Amazon Web Services, Inc. Accessed: Sep. 02, 2024. [Online]. Available: https://aws.amazon.com/what-is/cis-benchmarks/

[5] "Identity and Access Management in Cloud Security | CSA." Accessed: Sep. 02, 2024. [Online]. Available: https://cloudsecurityalliance.org/blog/2024/08/28/identity-and-access-management-in-cloud-security

[6] "GDPR - Amazon Web Services (AWS)," Amazon Web Services, Inc. Accessed: Sep. 02, 2024. [Online]. Available: https://aws.amazon.com/compliance/gdpr-center/

[7] A. Coos, "GDPR Data Encryption Requirements," Endpoint Protector Blog. Accessed: Sep. 02, 2024. [Online]. Available: https://www.endpointprotector.com/blog/gdpr-data-encryption-requirements

[8] "CIS controls can help you become compliant with the GDPR - Hitachi Systems Security." Accessed: Sep. 02, 2024. [Online]. Available: https://hitachi-systems-security.com/how-can-the-cis-controls-help-you-become-compliant-with-the-gdpr/

[9] “GDPR Incident Response Guidelines - BreachRx.” Accessed: Sep. 02, 2024. [Online]. Available: https://www.breachrx.com/global-regulations-data-privacy-laws/gdpr-guidelines/

[10] “Incident Response Policy Template for CIS Control 17.” Accessed: Sep. 02, 2024. [Online]. Available: https://www.cisecurity.org/insights/white-papers/incident-response-policy-template-for-cis-control-17

[11] “How does the CIS Controls framework align with IAM standards?” Accessed: Sep. 02, 2024. [Online]. Available: https://www.linkedin.com/advice/3/how-does-cis-controls-framework-align-iam-wkzaf

[12] “GDPR encryption: what you should know and what you do not know.” Accessed: Sep. 02, 2024. [Online]. Available: https://www.i-scoop.eu/gdpr-encryption/

[13] “Monitoring and Logging - Navigating GDPR Compliance on AWS.” Accessed: Sep. 02, 2024. [Online]. Available: https://docs.aws.amazon.com/whitepapers/latest/navigating-gdpr-compliance/monitoring-and-logging.html

[14] “Navigating GDPR Compliance on AWS - Navigating GDPR Compliance on AWS.” Accessed: Sep. 02, 2024. [Online]. Available: https://docs.aws.amazon.com/whitepapers/latest/navigating-gdpr-compliance/welcome.html

[15] “GDPR – A New Regulation,” CIS. Accessed: Sep. 02, 2024. [Online]. Available: https://www.cisecurity.org/blog/gdpr-a-new-regulation/