



EMERALD

Deliverable D6.3

Market analysis and applicability

Editor(s):	Björn Fanta (FABA)
Responsible Partner:	Fabasoft R&D GmbH
Status-Version:	Final – v1.0
Date:	30.04.2024
Type:	R
Distribution level (SEN, PU):	PU

Project Number:	101120688
Project Title:	EMERALD

Title of Deliverable:	Market analysis and applicability
Due Date of Delivery to the EC	30.04.2024

Work package responsible for the Deliverable:	WP6 - Dissemination, exploitation and communication
Editor(s):	Björn Fanta (FABA), Netsanet Haile Gebreyesus (IONOS)
Contributor(s):	FABA, IONOS, TECNALIA
Reviewer(s):	Juncal Alonso, Cristina Martinez (TECNALIA)
Approved by:	All Partners
Recommended/mandatory readers:	All working packages

Abstract:	Description of preliminary analysis of the market, by inspecting solutions, trends, and initiatives in the fields relevant to the project. Description of the preliminary analysis of standardization activities.
Keyword List:	Market, analysis, standardization, business application, competition
Licensing information:	This work is licensed under Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0 DEED https://creativecommons.org/licenses/by-sa/4.0/)
Disclaimer	Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. The European Union cannot be held responsible for them.

Document Description

Version	Date	Modifications Introduced	
		Modification Reason	Modified by
v0.1	15.02.2024	First draft version	FABA
v0.2	19.03.2023	Drafts of chapters 1, 2 and 3 added	FABA
v0.3	26.03.2024	Draft of chapter 5, contributions to chapter 2 and 3	FABA
v0.4	09.04.2024	Drafting and completion of chapters 2 and 3	FABA
v0.5	11.04.2024	Refining chapters 1, 2, 3 and 5	FABA
v0.6	18.04.2024	Adding chapter 4	IONOS
v0.7	22.04.2024	Finalizing document for final review, writing abstract	FABA
v0.8	23.04.2024	Internal QA review	TECNALIA
v0.9	29.04.2024	Addressed comments of internal QA review	FABA, IONOS
v1.0	30.04.2024	Submitted to the European Commission	TECNALIA

Table of contents

Terms and abbreviations.....	6
Executive Summary.....	8
1 Introduction.....	9
1.1 About this deliverable.....	9
1.2 Document structure.....	10
2 Market Analysis.....	11
2.1 Introduction and problem statement.....	11
2.2 The EMERALD Business Case.....	13
2.2.1 Building Trust.....	13
2.2.2 Why continuous/automated audits with supported evidence management?.....	14
2.2.3 EMERALD Value proposal.....	14
2.2.4 Customer segments.....	14
2.2.5 Target user’s personas.....	16
2.3 The EMERALD components.....	16
2.4 Potential Competition.....	19
3 Market Application.....	26
3.1 Initial SWOT analysis on the EMERALD value proposition.....	26
3.1.1 Strengths.....	26
3.1.2 Weaknesses.....	26
3.1.3 Opportunities.....	26
3.1.4 Threats.....	27
3.2 Addressing the SWOT in future work of EMERALD.....	27
4 Analysis of Standardization Activities.....	28
4.1 Processes related to Certification in Pilot Partners.....	28
4.2 Identified Challenges.....	29
4.2.1 Related to Assessment of Security Controls.....	29
4.2.2 Related to Aligning Certification Requirements.....	30
4.2.3 Suggested by Pilot Partners.....	32
4.3 Opportunities Presented by Standardization Initiatives.....	33
4.4 Collaboration with Standardization bodies.....	34
5 Conclusion.....	36
References.....	38
APPENDIX A: Links of additional competition findings.....	39
APPENDIX B: Survey on Standardization Requirements.....	40

List of tables

TABLE 1. CUSTOMER SEGMENTS.....	15
TABLE 2. TARGET USERS AND STAKEHOLDERS.....	16
TABLE 3. MAPPING OF EMERALD COMPONENTS TO KEY RESULTS AND THEIR TRL ADVANCEMENT	16
TABLE 4. MARKET SUMMARY.....	19
TABLE 5. KEY PLAYERS IN THE CLOUD SECURITY POSTURE MANAGEMENT COMPETITIVE LANDSCAPE	23
TABLE 6. EMERALD PILOT PARTNERS, SERVICES AND CURRENT CERTIFICATIONS	30
TABLE 7. CURRENT ENGAGEMENT IN STANDARDIZATION BODIES	34

List of figures

FIGURE 1. CLOUD SERVICE ADOPTION IN EUROPE. SOURCE: SYNERGY RESEARCH GROUP.....	12
---	----

Terms and abbreviations

AI	Artificial Intelligence
AMOE	Assessment and management of organizational evidence
API	Application Programming Interface
AWS	Amazon Web Services
BCP	Business Continuity Plan
BSI	Bundesamt für Sicherheit in der Informationstechnik
CaaS	Certification as a Service
CAB	Conformance Assessment Body
CCN	Centro Criptológico Nacional
CEN/CENELEC	European Committee for Standardization / European Committee for Electrotechnical Standardization
CI/CD	Continuous Integration / Continuous Delivery
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CPG	Consumer Packaged Goods
CSA or EU CSA	EU Cybersecurity Act
CSP	Cloud Service Provider
CSPM	Cloud Security Posture Management tool
DoA	Description of Action
EC	European Commission
ENISA	European Union Agency for Cybersecurity
ENS	Esquema Nacional de Seguridad
ETSI	European Telecommunications Standards Institute
EUCS	European Cybersecurity Certification Scheme for Cloud Services
GA	Grant Agreement to the project
GDPR	General Data Protection Regulation
GUI	Graphical User Interface
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IoT	Internet of Things
ISAE	International Standard on Assurance Engagements
ISMS	Information Security Management System
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
IT	Information Technologies
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
KR	Key Result
ML	Machine Learning
NIST	National Institute of Standards and Technology
NLP	Natural Language Processing
OSCAL	Open Security Controls Assessment Language
PaaS	Platform as a Service
PCI DSS	Payment Card Industry Data Security Standard
RDS	Relational Database Service
SaaS	Software as a Service
SARIF	Static Analysis Results Interchange Format
SME	Small and Medium Enterprise

SW	Software
SWOT	Strengths, Weaknesses, Opportunities, and Threats
TRL	Technology Readiness Level
UI/UX	User Interface / User Experience
XaaS	Anything as a Service
XML	Extensible Markup Language
XSLT	Extensible Stylesheet Language Transformations
YAML	Yet Another Markup Language

DRAFT

Executive Summary

This deliverable (D6.3) is an analysis of market potential, trends, stakeholders, and preparation of business scenarios that can be used when defining the exploitation strategies of EMERALD's commercial partners.

The main objective of EMERALD in this respect is to address future adoption of the proposed Certification as a Service (CaaS) approach and ensure the sustainability of the project results by considering the market trends, the business scenarios and the consortium and partners' needs and strategies.

The performed market analysis indicates that the trends are in favour for EMERALD and its findings are as of now gaining momentum in the Cloud Security area. It was also identified that EMERALD will create most of the value for stakeholders in security/risk management positions.

This deliverable will be further used as a guideline by the EMERALD partners in their innovation, exploitation and marketing efforts, as well as will be further used by WP6 to report the achieved results. Deliverables of WP5 – the four different pilots – are intricately linked to this deliverable.

D6.3 also addresses the first insights to standardization activities. The document presents an overview of the opportunities and challenges within the cloud industry regarding the implementation of standardization as a strategic approach for future exploitation of the outcomes of the EMERALD project. Additionally, it outlines actionable points for further steps and initiatives.

1 Introduction

The deliverable at hand has been created in WP6 of EMERALD, and is the first outcome of two tasks T6.2 and T6.4. Its contents will be further developed in upcoming deliverables in WP6 over the course of the project – especially for the exploitation strategy and the standardization activities.

What is the purpose of conducting a market analysis? This question is often posed by individuals seeking to establish a new business venture. Some may question the necessity of delving into abstract figures, uncertain forecasts, and complex economic terminology, favouring instead a more immediate approach to gaining experience. However, the importance of market analysis cannot be overlooked.

Undertaking a market analysis serves to provide a factual basis for a business concept:

- It enables the identification of market potential at an early stage, thereby aiding in the prevention of misguided decisions.
- Knowledge gaps can be readily identified and addressed in a timely manner.
- Existing products in the market can be assessed, allowing for differentiation strategies to be developed.
- Understanding competitors and predicting their potential reactions is made possible through a thorough analysis prior to market entry.

Within the realm of business planning, a market analysis holds considerable significance. Financial institutions are unlikely to provide loan support unless a comprehensive market analysis has been conducted. This analytical process is essential for aspiring entrepreneurs, as it forms the basis for strategic planning and successful marketing endeavours. A market analysis is fundamental for the realisation of a viable business proposition.

Key terminology associated with market analysis should be familiar to individuals embarking on this task. While the interpretation of such terms may not always be uniform, a foundational understanding is imperative for effective analysis. Essential terms include:

- **Market structure** (submarkets): organisational layout of the market, including factors such as regions, customer segments, product categories, and distribution channels.
- **Competitor analysis**: systematic evaluation of competitors to discern points of differentiation in products and services, as well as operational procedures.
- **Substitute products**: identification of potential alternative offerings that could impact demand and pricing dynamics, such as tea as a substitute for coffee.
- **Product life cycle**: phases of a product's lifespan, encompassing introduction, growth, maturity/saturation, and decline stages.

1.1 About this deliverable

The market analysis serves as a crucial decision-making tool for assessing the viability of potential products and services in the current and future market landscape. Once it is determined that a product or service has potential for success, the next step is to utilize the market analysis to formulate targeted marketing strategies. Some key advantages of conducting a market analysis include:

- **Identifying target demographics**: understanding which groups of individuals are interested in your product is essential for shaping an effective marketing approach. By analysing factors such as age, gender, and location of your target audience, you can tailor your advertising efforts accordingly.

- **Evaluating competitors:** by examining the offerings of competitors, you can identify your product's unique selling points and determine strategies for differentiation. Learning from the successes and failures of competitors can provide valuable insights for your own business strategy.
- **Enhancing the business plan:** incorporating data from the market analysis into your business plan demonstrates thorough planning and can bolster your credibility when seeking funding or loans.
- **Assessing market potential:** understanding the growth potential and trends in the market can help you anticipate future opportunities and challenges. By evaluating market margins and potential for optimization, you can better position your product for success and capitalize on market opportunities.

This deliverable will tackle these topics and prepare the upcoming exploitation strategies as well as the standardization activities of EMERALD.

Regarding standardization, the deliverable outlines the critical role of standardization in ensuring the success of the project. By standardizing processes and data involved in the cybersecurity certification process, EMERALD aims to enhance compatibility and interoperability with multiple European certification schemes. The document highlights the key standardization initiatives, such as the European Cybersecurity Certification Scheme for Cloud Services (EUCCS) and the Open Security Controls Assessment Language (OSCAL) to align with industry best practices. Insights from pilot partners and industry research underscore the importance of standardization in streamlining the certification process for cloud providers, fostering trust, credibility, and usability of cybersecurity certifications. The document emphasizes the strategic collaboration with standardization bodies to ensure seamless integration with diverse certification frameworks, ultimately empowering cloud providers to achieve and maintain continuous certification with confidence and efficiency.

1.2 Document structure

This deliverable covers in Section 2 the topics of the actual market analysis in a brief and condensed way for EMERALD, listing the problem statement, value proposition and potential customer segments.

The next chapter, Section 3 - Market application, covers the issues of transferring the results and findings of EMERALD into real products and services and prepares for the upcoming exploitation strategy parts of EMERALD. Because of the nature of this first surveying deliverable this chapter is also a very brief listing of the state of play and possible options.

The third part of this deliverable tackles in Section 4 the first view on standardization activities for the EMERALD consortium and prepares for the future standardization strategy parts and activities.

The deliverable finishes with a short conclusion (Section 5), stating the future work for the upcoming months of EMERALD and gives a perspective for the time beyond EMERALD as a funded project – which is the core of a sound exploitation strategy for an EU funded project.

The document also contains two appendices: *APPENDIX A: Links of additional competition findings*, addressing an additional collection of potential competition, and *APPENDIX B: Survey on Standardization Requirements* that provides the survey for the standardization questionnaire.

2 Market Analysis

To begin the analysis, it is important to acquaint with the market that pertains business potentials for EMERALD. It is possible to identify these by considering the following questions:

- What is the problem that the products or services address?
- What is the offered value proposition?
- What are possible market or customer segments?
- What preferences do these target segments have?

The following pages will address these questions in general and set the scene for the situation EMERALD is facing. The document will prepare the future exploitation and standardization activities of the consortium by doing so.

Information about the market can be gathered from various sources such as online resources, trade publications, chambers of commerce, industry associations, market research firms, government statistical agencies, and company financial reports. For this deliverable, the EMERALD consortium will make use of internet research, knowledge of different working groups the partners are active in and statements from the pilot partners (customer segment).

2.1 Introduction and problem statement

In recent years, there has been a significant increase in businesses utilizing cloud-based services and applications, both in Large Enterprises and Small and Medium Enterprises (SMEs). According to recent Eurostat statistics¹, the adoption of cloud computing has risen by approximately 21 percentage points in large enterprises since 2014. This includes not only basic services like file storage and email systems, but also more advanced cloud-based services such as financial and accounting software applications, customer relationship management, and utilizing computing power for business applications. As a result, cloud-based services have evolved into complex ecosystems, incorporating virtual infrastructure, business processes, and application code. These advanced services increasingly incorporate Artificial Intelligence (AI) technologies like Machine Learning (ML) and Natural Language Processing (NLP), further adding to their complexity. This has led to a need for a more agile certification process for cloud-based services, such as continuous monitoring and assessment as outlined in the certifications of the EU Cybersecurity Act (EU CSA)². While agile development methodologies have helped reduce time-to-market for new applications, there are still challenges that must be addressed to fully leverage the European Digital Single Market strategies.

Although there has been proof of concepts for continuous monitoring and assessment, there are interoperability challenges due to the variety of technologies being used. The lack of integration of different sources results in a mix of assessment tools and formats. While the Open Security Controls Assessment Language (OSCAL)³ addresses this issue, it is not yet widely adopted. As a result, the current landscape appears fragmented, like a puzzle that could be unified with effort to create a seamless platform for data and services.

From a business perspective, there remains a significant barrier to entry for small and medium-sized enterprises (SMEs) looking to engage in cloud computing. This barrier affects both SMEs as users of cloud services and as service providers. For SMEs as consumers, cloud computing

¹ Eurostat from 2018: https://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises

² <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act>

³ <https://github.com/usnistgov/OSCAL> , <https://csrc.nist.gov/Projects/Open-Security-Controls-Assessment-Language>

holds the potential for substantial benefits as the services offered often provide functionality and security beyond what they could achieve on their own. However, there is still apprehension around moving to the cloud due to concerns about data breaches, especially since SMEs may lack security expertise within their teams.

On the other hand, SMEs operating as service providers, particularly those focused on specialized functions or niche markets, face challenges related to visibility, interoperability, and security when dealing with larger cloud providers in the enterprise sector. The introduction of industry-specific regulations, like those in the AI-Act⁴, adds to the complexity by requiring compliance with various security standards. Efforts to increase the reusability of audit evidence could streamline certification processes and reduce the time and resources needed for compliance.

The current landscape shows – as mentioned – a fragmentation of certification schemes in the cloud computing sector, underscoring the need for a unified approach. The forthcoming European Cybersecurity Certification Scheme for Cloud Services (EUCS)⁵ aims to address this issue. Despite the growing adoption of cloud, edge computing, and IoT technologies in recent years, large companies in highly regulated industries, such as finance, face additional challenges. These challenges stem from the diverse technologies being used and the stringent security, privacy, and legal requirements that must be met across different environments.

For companies in regulated industries, integrating new services, ensuring compliance, and managing security and privacy can be complex and costly. In the financial sector, concerns about outsourcing IT services include maintaining control, addressing evolving threats, and optimizing resource utilization. Uncertainties surrounding the migration to cloud computing continue to hinder adoption of the technology, particularly among companies in highly regulated sectors.

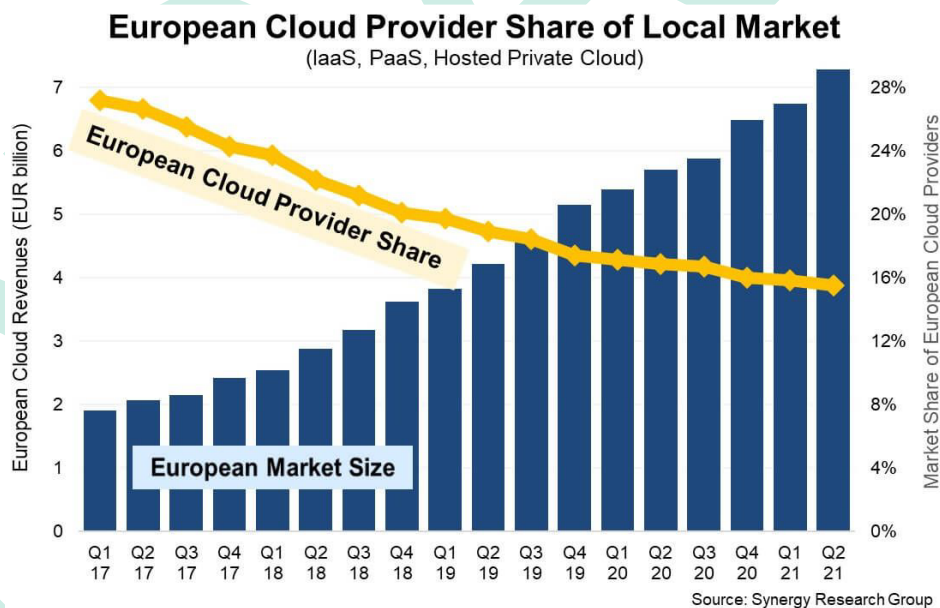


Figure 1. Cloud service adoption in Europe. Source: Synergy Research Group

Finally, due to the ever-changing nature of the cloud industry, it is imperative for professionals to maintain a dynamic perspective on the subject. What was once considered a secure and suitable service may not meet the required standards over time. In addition, external factors

⁴ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>

⁵ <https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme>

such as cyber-attacks or security breaches may compel developers or operations teams to transfer services or data from one provider to another. Currently, the lack of efficient interfaces, real-time monitoring systems, and quick response mechanisms results in a labour-intensive and expensive process. Therefore, it is crucial to develop new strategies that promote self-adaptability of services and enable the easy transfer of data to assist developers in creating and implementing secure services.

2.2 The EMERALD Business Case

The business case for EMERALD will be collaboratively developed with EMERALD partners in a later stage of the project and documented in the deliverables D6.6 [1] and D6.7 [2]. For now, only a high-level overview is being presented in this section.

2.2.1 Building Trust

European Cloud Service Providers encounter various obstacles in establishing trust with customers for their cloud services. The current certification schemes in the market are diverse, with the ISO/IEC 27001 scheme being the most prominent. However, other schemes, especially national frameworks, have not been as widely adopted. The European certification on cloud services (EUCS) seeks to address this issue by offering a certification that is recognized throughout Europe, thereby reducing fragmentation in the market. This initiative presents an opportunity for providers to tap into a new market segment. Another issue in the certification schemes market pertains to security controls. Each scheme is tailored to address specific requirements, necessitating different security controls. For a Cloud Service Provider aiming to comply with multiple schemes, this would entail undergoing multiple audits to satisfy the requirements of each standard. The EU-SEC project⁶ was established to address this challenge and developed a comprehensive list of Security Controls to allow for the selection of a suitable subset. However, the challenge of reusing evidence persists. One of the key challenges faced by European cloud providers when pursuing certification is the selection of a Conformity Assessment Method. There are various practices available, including ISO-based, ISAE-based, self-assessment, and evidence-based approaches, each with their own unique scope, depth, and processes. This can lead to a lack of trust and confusion among consumers.

The solution to these challenges has been delegated to the European Union for Cybersecurity (ENISA) under the Cybersecurity Act⁷. However, ENISA itself has encountered difficulties as there is currently no specific framework for cloud certification, nor are there tools or methods available to support the recommended security controls, assurance levels, or conformity assessment methods required by the Cybersecurity Act. In order to address these gaps, ENISA had established a specialized working group⁸ tasked with defining the European certification for cloud services (EUCS).

EMERALD aims to leverage the results and findings of the MEDINA project⁹ to offer a cutting-edge Certification-as-a-Service approach and toolset to assist CSPs (Infrastructure as a Service, Platform as a Service, and Software as a Service providers) in obtaining continuous cloud security certifications using reliable evidence-management techniques. Specifically, EMERALD will support CSPs in achieving certification status in line with the EU Cybersecurity Act, the European

⁶ <https://www.sec-cert.eu/>

⁷ <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act>

⁸ https://www.enisa.europa.eu/topics/certification/copy_of_adhoc_wg_calls/ahWG02

⁹ <https://medina-project.eu/>

Cybersecurity Certification Scheme, the BSI C5¹⁰ and explore approaches towards sets of requirements given by Cloud customers like CaixaBank or emerging AI schemes like the BSI AIC4¹¹.

2.2.2 Why continuous/automated audits with supported evidence management?

Certifications obtained on an annual basis are no longer meeting the needs of high-level cloud customers, such as those in the finance and government sectors. These customers are seeking a continuous assurance service instead of traditional point-in-time auditing. Continuous auditing can be defined as a method of continuously measuring specific attributes of an information system and comparing them to established security objectives. The results of this ongoing auditing process are shared in real-time with customers in a manner that protects the confidentiality of the cloud provider's operations. Continuous auditing, utilizing innovative and automated tools to conduct surveillance audits at regular intervals, is now necessary in order to keep pace with rapidly advancing technology. Today's rapidly evolving technology landscape has made traditional auditing practices obsolete. The widespread adoption of DevOps principles, including continuous integration and deployment, has led to frequent changes in production environments, making traditional auditing methods ineffective.

2.2.3 EMERALD Value proposal

Value proposal: *Continuous cybersecurity cloud certification as a Service.* [3]

Supporting such proposal by a seamless user experience for continuous cybersecurity certification, based on next generation gathering tools and reducing complexity in multi-scheme Cloud certifications. Offering a uniform way to address audits and offering a solid degree of complexity reduction through the customization of the audit process.

This value proposal is addresses different stakeholders, as mentioned in the EMERALD DoA [3]:

- For cloud service providers as well as cloud customers, EMERALD offers a framework to set-up, manage, and monitor their certifications and enable lean re-certification.
- For auditors, EMERALD is an audit assistance framework.
- For cybersecurity and standardization agencies, EMERALD provides novel strategies and methods for building cybersecurity requirements and metrics that can react to changes and, if necessary, are interoperable enough to be translated to other schemes.
- For companies providing solutions of cybersecurity, the EMERALD tools allow to improve current tools or diversify business.

2.2.4 Customer segments

Closely associated with the competitive analysis is the examination of sectors that generate the highest revenue. By evaluating the attractiveness and structure of these sectors within your defined market, valuable insights can be gained into the target demographics. This analysis can help derive marketing strategies based on customer requirements and behaviour. Key questions to consider include:

- What are the sales figures in the respective industry?

¹⁰ https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html

¹¹ <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/AIC4/aic4.html>

- What emerging trends are present in the industry?
- Which recent innovations have contributed to the industry's success?

The EMERALD main approach consists of four steps:

1. Select a certification scheme and utilize an intelligent system to identify metrics for demonstrating compliance.
2. Extract knowledge from various layers of the cloud service and prepare relevant evidence.
3. Establish an evidence graph to consolidate information for queries.
4. Assess chosen metrics based on certification graph information and provide interoperability with other assessment tools throughout the cloud service lifecycle.

The EMERALD mission [3] can be summarized as the following:

Building upon the success of the H2020 project MEDINA, EMERALD aims to advance findings to TRL 7 starting in summer 2023. The focus will be on evidence management components and two proofs of concept for composite certification and AI-certification schemes.

The EMERALD overall objective and rationale is [3]:

EMERALD aims to develop Certification-as-a-Service (CaaS) for continuous certification of harmonized cybersecurity schemes like EUCS. Stakeholders in the cybersecurity domain, including cloud service providers, customers, auditors, and agencies, will benefit from a framework for managing and monitoring certifications, facilitating lean re-certification, and providing audit assistance. EMERALD will also offer strategies for building cybersecurity requirements and metrics that are responsive to changes and interoperable with other schemes.

Keeping this information in mind, the different customer segments foreseen as beneficiaries of the EMERALD's value proposition are listed in the following Table 1, which also offers a brief description and potential access channel for each stakeholder (segment).

Table 1. Customer segments

Customer segment	Description	Companies
Cloud service providers	IT company that provides XaaS services to customers	Fabasoft, IONOS, CloudFerro, ONS, AWS, IBM, HPE, MS Azure, Google Cloud, ...
Cloud customers	Customer who makes use of XaaS services, offered by Cloud service provider companies	CXB, Bosch, Siemens, ...
Auditors	Expert instance accredited to perform the actual audit or verify the set-up future CaaS approaches within companies	NIXU, TECNALIA Certification, PwC, KPMG, DEKRA, ...
Standardization agencies	Scheme owners	ENISA, ETSI, CEN-CENELEC, BSI Germany, ...

Customer segment	Description	Companies
Companies in the cybersecurity field	Companies with expert knowledge, able to contribute to CaaS life-cycles or the tooling landscape	Potential Cluditor Spin-Off, Arthur's Legal, Cadzow Communications, ...

2.2.5 Target user's personas

EMERALD – like MEDINA – is targeted to help Cloud Service Providers, Cloud Service users and both internal and external Auditors, including Conformity Assessment Bodies (CABs) to meet security requirements that arise from their specific needs. EMERALD is intended to be used by users with different roles, i.e., personas, which are briefly described in Table 2. Each Role is assigned set of responsibilities in the CSP organisation.

Table 2. Target Users and Stakeholders

Role Persona	Description
Compliance Manager	Responsible for the implementation of the Security Control Frameworks
	Responsible for the correct implementation of the internal controls
	Responsible for incident management
Chief Information Security Officer (CISO)	Responsible for security in the company, chooses what Security Controls should be implemented
Internal Control Owner (ICO)	Responsible for creating the internal controls
	Executing the internal controls
Auditor	Performs all actions required to audit a Company
	Responsible for performing internal audits

2.3 The EMERALD components

Table 3 lists the different components in the EMERALD tooling landscape and connects them with the respective key result and responsible partner, as referenced in the EMERALD DoA [3]. The short description gives an insight of what specific topic or challenge the component addresses within the EMERALD value proposition. The Information on starting TRL and ending TRL is also given in this table for future reference of upcoming WP6 deliverables, so that the exploitation strategy can plan according to this information.

Table 3. Mapping of EMERALD components to Key Results and their TRL advancement

Tools in EMERALD	Component Name	Partner	Start TRL	End TRL	Enhancements in EMERALD
Compliance core	Cluditor	FHG	5	7	Integrate additional evidence collecting techniques into the Cluditor, especially by integrating the knowledge graph into Cluditor Orchestrator. Extend Cluditor Discovery with modules related to the discovery of information from CI/CD templates.
	Trustworthiness System (TWS)	TECNALIA	5	7	Provide interoperability with the European Blockchain Services Infrastructure (EBSI)

Tools in EMERALD	Component Name	Partner	Start TRL	End TRL	Enhancements in EMERALD
Standards & data core	Requirement Mapping Assistant (RMA)	CNR	3-4	5-6	Enhance functionalities by 1) exploring strategies for metrics association, 2) optimizing the returned metrics, 3) mapping of requirements of different schemes.
	Repository of Controls and Metrics (RCM)	TECNALIA	3-4	7	Interoperability with exchange formats, such as OSCAL. Provide automatic mechanisms to update the catalogues and support multi scheme and multi-level certification.
Evidence management core	AMOE	FABA	3-4	5-6	Improve evidence extraction quality and prepare plus integrate extracted information to the certification graph for verification of technical implementation of organisational measures.
	CODYZE - a static code analysis tool	FHG	4-5	6-7	Improve chain of reasoning for verification results. Revise modelling language for more generic composition of rules. Implement automated rule inference and promote system-level compliance validations using Cloud Property Graph. Enhance compliance coverage by supporting more standards and providing checks for AI-based systems.
	eKNOWS - software analysis platform	SCCH	4-6	5-7	Extend generic components for business rule extraction for domain-specific rule and constraint localization. Extend generic components for model guided symbolic execution use-case specific compliance checks and fact extraction. Provide integration of analysis results in the certification graph.
	AI-SEC - AI Security Evidence Collector	FHG	3-4	5-6	Make previously isolated techniques from research applicable in productive environment and jointly assess ML models.
UI	EMERALD UI/UX - a concept by KNOW,	KNOW/ FABA	5	6-7	Integrate the previously isolated UIs of the MEDINA tools into one UI/UX that is tailored to the needs of the target users.

Tools in EMERALD	Component Name	Partner	Start TRL	End TRL	Enhancements in EMERALD
	implemented by FABA				

A more detailed discussion on the tools adopted in EMERALD is listed below:

Clouditor - an Open-Source micro-service-based cloud assurance tool developed by FHG. It consists of several components that take care of the discovery of cloud resources, the assessment of resources based on logic-based rules and the overall orchestration of different aspects of Cloud certification. Clouditor is the reference implementation of several MEDINA components, such as the MEDINA Orchestrator [4], and its framework powers the Continuous Automated Monitoring (CAM) component of the Gaia-X Federation Services¹².

Trustworthiness System (TWS) - a mechanism, developed by TECNALIA, for secure long-term storage of evidence and assessment results. It is backboned by a Blockchain network, strengthening the security level in terms of integrity, availability, etc., by providing the trustworthiness functionalities by means of Smart Contracts. Usability is also considered essential through a graphical Blockchain viewer providing a user-friendly way of extracting information content from the Blockchain.

Requirement Mapping Assistant (RMA) - an intelligent system that will leverage state-of-the-art Artificial Intelligence (AI) techniques for performing its operation. It will be developed starting from the Metric Recommender available in the MEDINA project [4], which is a prototype tool able to associate a set of metrics to a requirement taken from a certification scheme, by leveraging NLP techniques for the requirement and metric representation.

Repository of Controls and Metrics (RCM) – based on the MEDINA component “Catalogue of controls and metrics” [4], is an IT tool for the storage and management of controls, requirements, metrics, and their relationships. It supports the endorsement of Security Control Frameworks and related attributes: security requirements, categories, controls, reference TOMs, metrics, evidence, and assurance levels; and provides guidance for the (self-) assessment of the requirements.

AMOE - the MEDINA based component [4] “Assessment and Management of Organisational Evidence” is a proof of concept to address parts of security requirements of organisational nature, developed by FABA. The focus of the component is to enable evidence extraction from policy documents that are essential to cover some parts of the requirements. The tool is able to provide assessment hints based on special metrics defined for the component.

CODYZE - a static code analysis tool developed by FHG. It verifies compliance of a software implementation to security standards and certification schemes. It operates on a CPG and queries source code properties critical for compliance such as API calls to third party libraries. It uses a domain specific language to define rules specifying what values code properties must have to be compliant. Rule sets are defined for specific software libraries covering multiple use cases. Mappings between rules and requirements from standards and certification schemes define how validated source code property affirm compliance. A report in the SARIF¹³ format lists the results of each rule evaluation. These results supply basic evidence why a rule has evaluated as compliant or non-compliant.

¹² <http://gitlab.com/gaia-x/data-infrastructure-federation-services/cam>

¹³ <https://docs.oasis-open.org/sarif/sarif/v2.1.0/sarif-v2.1.0.html>

eKNOWS - is a software analysis platform developed by SCCH. The platform supports rapid development of multi-language software analysis tools from pre-built analysis components, which build on a technology agnostic generic layer and are extended to meet use case-specific requirements.

AI-SEC - the FHG AI Security Evidence Collector will analyse ML and AI models for several key evidence regarding robustness against adversarial attacks, explainability and fairness. To achieve this, AI-SEC aggregates existing, but isolated techniques from research and combines them for holistic evidence collection of AI models.

EMERALD UI/UX - a concept by KNOW, implemented by FABA, bringing together the target groups and technology providers. The aim is to develop a reliable, explainable and trustworthy UI/UX that addresses the CaaS approach of EMERALD. It builds upon the concepts defined in the Unified UI and Company Compliance Dashboard (developed by FABA) of MEDINA [4].

2.4 Potential Competition

Table 4 provides an analysis of existing tools and sources relevant for EMERALD, including their (functional) description. This is an initial version of the market analysis, which will be enlarged in upcoming deliverables. An additional assembly of links for potential competition is also given in *APPENDIX A: Links of additional competition findings* of this document.

Table 4. Market summary

Solution/tool name	Solution's description
ISO/IEC 19086-4 (Cloud Security Service Level Agreements) ¹⁴	ISO/IEC 19086-4 (Cloud Security Service Level Agreements), provides a non-certifiable set of quantitative/qualitative service level objectives for CSPs
Reference document on security measures for Operators of Essential Services ¹⁵	Reference implementations of organizational and security measures in critical infrastructures
CIS Controls ^{TM16} and CIS Benchmarks ^{TM17} Control list ¹⁸	Reference implementations of organizational and security measures for several controls, with examples for various CSPs
Azure Security Benchmark ¹⁹	Reference implementations of organizational and security measures for Azure
NIST- Performance Measurement Guide for Information Security Draft of the Second version (September 2020) ²⁰	Metrics implementations

¹⁴ <https://www.iso.org/standard/68242.html>

¹⁵ https://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document_security_measures_0040C183-FF20-ECC4-A3D11FA2A80DAAC6_53643.pdf

¹⁶ <https://www.cisecurity.org/controls/>

¹⁷ <https://www.cisecurity.org/cis-benchmarks/>

¹⁸ <https://www.cisecurity.org/controls/cis-controls-list/>

¹⁹ <https://docs.microsoft.com/en-us/security/benchmark/azure/>

²⁰ <https://csrc.nist.gov/publications/detail/sp/800-55/rev-2/draft>

Solution/tool name	Solution's description
AWS- Best Practices for Security, Identity, & Compliance ²¹	Reference implementations of organizational and security measures for AWS
Compliance validation for Amazon RDS ²²	Reference implementations of organizational and security measures for Amazon RDS
PRISMA TM ²³	<p>The Prisma suite secures a public cloud environment, SaaS applications, internet access, mobile users, and remote locations through a cloud-delivered architecture. It is a comprehensive suite of security services to effectively predict, prevent, detect, and automatically respond to security and compliance risks without creating friction for users, developers, and security and network administrators. The suite is composed by:</p> <ul style="list-style-type: none"> • Prisma Cloud. Cloud application security (redlock) • Prisma Access (SASE). Cloud access security • Prisma SaaS. SaaS application security • Prisma SD-WAN. Solution that enables the cloud-delivered branch • VM-Series. Cloud-native security • CN-Series. Solution that helps to secure Kubernetes environments with the CN-Series Firewall
TIC – CCN Security Guidelines Cloud services usage (Spanish) ²⁴	Reference implementations of organizational and security measures for Spanish ENS, including examples from several CSPs
RSA Archer ^{25, 26}	<p>Platform for managing integrated risk management program. It can:</p> <ul style="list-style-type: none"> • Manage policies, controls, risks, assessments, and deficiencies. • Automate business processes • Deliver real-time reports • On premise or host (SaaS) • Integration with external systems to support data analysis, process management and reporting
Neupart Secure ISMS ²⁷	Secure ISMS is an information security management system that enables organisations to efficiently manage IT risks and compliance requirements, such as ISO 27001/2, EU Data

²¹ https://aws.amazon.com/products/security/?nc1=h_ls

²² <https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/RDS-compliance.html>

²³ <https://docs.paloaltonetworks.com/prisma.html>

²⁴ <https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/541-ccn-stic-823-seguridad-en-entornos-cloud/file.html>

²⁵ <https://www.rsa.com/content/dam/en/data-sheet/rsa-archer-grc-platform.pdf>

²⁶ <https://www.rsa.com/de-de/products/integrated-risk-management/archer-platform>

²⁷ <https://www.neupart.com/products>

Solution/tool name	Solution's description
	<p>Protection Regulation and PCI DSS. It includes the following packages:</p> <ul style="list-style-type: none"> • Secure ISMS Risk: Includes risk treatment, business impact assessments, vulnerability analysis, Static and dynamic reports, amongst others. • Secures ISMS Compliance: Manage those tasks that are part of an ISO 27001 Information Security Management. • Secure ISMS BCP, Business continuity plans availability. <p>Some other characteristics:</p> <ul style="list-style-type: none"> • On premise or host (SaaS) • GDPR package also available
<p>US NIST's OSCAL²⁸</p> <p>OSCAL Catalog Model²⁹</p> <p>OSCAL tools³⁰</p>	<p>OSCAL is an Open Security Controls Assessment Language created by the NIST, that is a set of formats expressed in XML, JSON and YAML.</p> <p>The OSCAL Catalog Model represents a collection of controls, represented as a control catalogue. The OSCAL Catalog Model has been designed to represent security and privacy controls in standardized, machine-readable formats. The OSCAL catalog model standardizes the representation of control definitions from various sources (e.g., SP 800-53, ISO/IEC 27002, COBIT 5) allowing control information to be easily searched, imported, and exported by applications using a generic format.</p> <p>Some open-source tools are also available:</p> <ul style="list-style-type: none"> • OSCAL java library • XSLT Tooling • OSCAL KIT • OSCAL GUI
<p>Azure Policies³¹</p>	<p>Azure Policy is a service in Azure which allows to create polices which enforce and control the properties of a resource. When these policies are used, they enforce different rules and effects over the resources of a company, so those resources stay compliant with the companies' IT governance standards. Azure policy has three components:</p> <ul style="list-style-type: none"> • Policy definition that represents the conditions to be controlled • Policy assignment is the scope of what the policy definition can take effect around • Policy parameters

²⁸ <https://pages.nist.gov/OSCAL/>

²⁹ <https://pages.nist.gov/OSCAL/documentation/schema/catalog-layer/catalog/>

³⁰ <https://pages.nist.gov/OSCAL/tools/>

³¹ <https://docs.microsoft.com/en-us/azure/governance/policy/overview>

Solution/tool name	Solution's description
	Through its compliance dashboard, it provides an aggregated view to assess the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity.
AWS ConfigRules ³² Page 292 of the pdf ³³	An AWS Config rule represents an AWS Lambda function that it is created for a custom rule or a predefined function for an AWS managed rule. The function evaluates configuration items to assess whether the AWS resources comply with the desired configurations. This function can run when AWS Config detects a configuration change to an AWS resource and at a periodic frequency (for example, every 24 hours).
Divvycloud ³⁴	Set of solutions to protect cloud (multi-cloud) and container environment from misconfigurations, policy violations, threats and IAM Challenges by using automation and real-time remediation to ensure continuous security and compliance. DivvyCloud supports AWS, Microsoft Azure, Google Cloud Platform, Alibaba Cloud, and Kubernetes.
RedLock or PRISMA CLOUD TM ³⁵	Prisma™ Cloud is a cloud native security platform that enables cloud security posture management (CSPM) and cloud workload protection platform (CWPP) for comprehensive visibility and threat detection across an organization's hybrid, multi-cloud infrastructure. Prisma Cloud taps into the cloud providers' APIs for read-only access of the network traffic, user activity, and configuration of systems and services, and correlates these disparate data sets to help the cloud compliance and security analytics teams prioritize risks and quickly respond to issues. It also uses an agent-based approach to secure the host, container, and serverless computing environments against vulnerabilities, malware, and compliance violations.
Cloudcheckr ³⁶ Datasheet of cloudcheckr ³⁷	Cloudcheckr CMx™ is an extensible and scalable cloud management software that enables total visibility into infrastructures and organizational management (by individuals, roles and teams). It unifies cloud data from sources all over the enterprise. It has the following features. <ul style="list-style-type: none"> • Cost management. • Invoicing: Allocate cloud charges according to the business requirements.

³² https://docs.aws.amazon.com/config/latest/APIReference/API_ConfigRule.html

³³ https://docs.aws.amazon.com/config/latest/APIReference/awsconfig-apiref.pdf#API_ConfigRule

³⁴ <https://divvycloud.com/>

³⁵ <https://docs.paloaltonetworks.com/prisma/prisma-cloud.html>

³⁶ <https://cloudcheckr.com/products/cm/>

³⁷ <https://click.cloudcheckr.com/rs/222-ENM-584/images/CloudCheckr-CMx-Datasheet.pdf>





Solution/tool name	Solution's description
	<ul style="list-style-type: none"> Security and compliance: Ensure compliance and prevent misconfigurations that lead to costly security breaches.
AWS Audit Manager ³⁸	<p>AWS Audit Manager is a solution that helps to continuously audit the AWS usage to simplify the assess risk and compliance with regulations and industry standards. Audit Manager automates evidence collection to reduce the “all hands-on deck” manual effort that often happens for audits and enable to scale the audit capability in the cloud as a business grows.</p> <p>It provides tools to assess if the policies, procedures, and activities or controls are operating effectively, it also includes features to manage stakeholder reviews of the controls and to build audit-ready reports with much less manual effort.</p>
Cloud Security Alliance	<p>Cloud Security Alliance (CSA) is a not-for-profit organization with the mission to “promote the use of best practices for providing security assurance within cloud computing, and to provide education on the uses of cloud computing to help secure all other forms of computing.” (Wikipedia)</p> <p>CSA published “The Continuous Audit Metrics Catalog” for compliance managers in October 2021. The catalogue covers topics of security metrics and continuous auditing and this work is closely linked to EMERALD catalogue of controls and metrics. The key take-away is that security metrics need to be designed carefully so that they enable automation i.e., continuous assurance.</p> <p>The metrics in the CSA catalogue aim to support internal CSP governance, risk, and compliance (GRC) activities and provide a helpful baseline for service-level agreement transparency</p>

Additionally, EMERALD is highly related to the Cloud Security Posture Management (CSPM) market. Hence, special attention will be given to the CSPM market, starting in Table 5.

Table 5. Key players in the Cloud Security Posture management competitive landscape

Player	Key message
	<p>VerSprite developed the Cloud Security Assessment Platform (CSAP) to support our cloud security assessments and analysis. Our enterprise-ready cloud platform provides visual reporting in a way that makes cloud security easy to manage and prioritize risks.</p> <p>By providing organizations with a comprehensive view of their security posture, CISOs and security leaders now have a clear</p>

³⁸ <https://aws.amazon.com/es/audit-manager/>

Player	Key message
	<p>visibility into how their overall cloud environment is positioned against standard security framework.</p> <p>VerSprite's risk-based threat modelling process allows our security consultants to not only discover, analyse, and report on an organization's CSP hosted infrastructure, but also assess security risks and their related business impact. CSAP is delivered via a SaaS model where the only connection to the client's environment is via read-only 'audit' role.³⁹</p>
	<p>The Cloud Security Posture Management (CSPM) previously known as Cloud Infrastructure Security Posture Assessment was defined in response to the growing need of organizations to correctly configure public cloud IaaS and PaaS services and address cloud risks. CSPM is a class of security tools as defined by Gartner include use cases for compliance monitoring, DevOps integration, incident response, risk assessment, and risk visualization.⁴⁰</p>
 Falcon Horizon CSPM	<p>Cloud security posture management (CSPM) automates the identification and remediation of risks across cloud infrastructures, including Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS). CSPM is used for risk visualization and assessment, incident response, compliance monitoring, and DevOps integration, and can uniformly apply best practices for cloud security to hybrid, multi-cloud, and container environments.⁴¹</p>
	<p>Zscaler Cloud Security Posture Management (CSPM) automatically identifies and remediates application misconfigurations in SaaS, IaaS, and PaaS to reduce risk and ensure compliance. Zscaler CSPM is part of the comprehensive, 100% cloud-delivered data protection capabilities in the Zscaler Cloud Security Platform.⁴²</p>
 Aqua Security	<p>Scan, monitor and remediate configuration issues in public cloud accounts according to best practices and compliance standards, across AWS, Azure, Google Cloud, and Oracle Cloud.⁴³</p>




³⁹ <https://versprite.com/security-resources/cloud-platform-demo/>

⁴⁰ <https://www.fugue.co/cloud-security-posture-management>

⁴¹ <https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-security-posture-management-cspm/>

⁴² <https://www.zscaler.com/products/cloud-security-posture-management>

⁴³ <https://www.aquasec.com/products/cspm/>

Player	Key message
	<p>OpsCompass captures a high-fidelity snapshot of your entire cloud and all its configurations, creating a complete picture of your environment. From this snapshot, it generates a proprietary score and helpful graphs for your dashboard that indicate how you are performing against key compliance standards and identify compliance trends at a glance. You can then drill down to discover exactly where any compliance problems lie and how you can fix them.⁴⁴</p>
 <p>CloudCheckr CMx High Security</p>	<p>CloudCheckr CMx High Security is built to the highest levels of security and supports 300 rigorous controls in 17 control families from NIST 800-53. Combined with AI-based threat detection and daily automated internal vulnerability scans, our commercial-grade cloud computing security management will accelerate your cloud adoption in financial services, healthcare, and other regulated industries. With emerging public cloud security challenges, get started with CMx High Security today to achieve cloud regulatory compliance, security compliance, and the optimal protection of your data.⁴⁵</p>
 <p>CloudGuard</p>	<p>CloudGuard Cloud Security Posture Management, part of the CloudGuard Cloud Native Security platform, automates governance across multi-cloud assets and services including visualization and assessment of security posture, misconfiguration detection, and enforcement of security best practices and compliance frameworks.⁴⁶</p>

⁴⁴ <http://www.opscompass.com/>

⁴⁵ <https://cloudcheckr.com/>

⁴⁶ <https://www.checkpoint.com/products/cloud-security-posture-management/>

3 Market Application

As a founder, it is crucial to anticipate the future development of the market. As EMERALD is in its very early stage and – due to its research nature – still has a good amount of uncertainty in its composition of solutions. This document will kick-off the market application topic with a preliminary market potential analysis that should address concerns such as potential staffing needs, market entry obstacles (e.g., costs), key success factors, and upcoming market trends.

3.1 Initial SWOT analysis on the EMERALD value proposition

The – as of early 2024 – best approach to kick-off this topic is to conduct a small SWOT analysis and raise awareness to the project teams towards the strengths, weaknesses, opportunities and threads of and for EMERALD.

It is noteworthy that later on in the project, it will become necessary to conduct further and more detailed research on the market application for each component and the overall EMERALD CaaS approach in general (see chapter 3.2) – this will be done in D6.6 [1] and D6.7 [2] of EMERALD.

3.1.1 Strengths

The EU project EMERALD has several strengths, among them the goal of automated certification; EMERALD aims to enable the automated certification of cloud-based services. Currently, this process is manual, but EMERALD aims to provide faster and continuous certification through Certification-as-a-Service. Additionally, certification proves the security and functionality of cloud-based services and EMERALD aims at enhancing transparency and trust for providers and customers.

A core strength of EMERALD is also the level of collaboration and expertise. EMERALD works with research partners to utilise approaches from the MEDINA project and builds upon elaborated concepts. This collaboration enables a successful development of a solution for automated certification.

3.1.2 Weaknesses

Navigating cloud certification can be quite the journey. It's a complex process that involves continuous and automated certification of cloud-based services. With so many different services to consider and rapid development happening all the time, it's important to coordinate carefully.

When it comes to tackling cyber security issues it becomes clear that these challenges are global, and that international cooperation is key. While initiatives like EMERALD can make significant progress, the EU can't do it alone. Working together with other countries is essential for real change.

Introducing a new certification solution isn't just about the technical side of things. It also requires buy-in and active participation from suppliers, customers, auditors, and standardization bodies. Getting everyone on board and actually implementing the solution can be a challenge, but it's worth it in the end.

3.1.3 Opportunities

Three main dimensions open up opportunities in EMERALD:

- Standardisation and comparability: EMERALD advocates for process standardisation and content comparability in cloud certification.

- Integrating concepts: EMERALD is in the process of creating a Certification-as-a-Service solution that integrates concepts such as evidence management, compliance, standards, data, and a user-friendly interface.
- Promoting data-driven behaviour: EMERALD leverages data analytics to support data-driven decision-making in the realm of cyber-security.

3.1.4 Threats

One of the main challenges facing EMERALD is actually one of its biggest strengths - collaboration. With so many partners involved and different interests to navigate, being part of an EU project can sometimes feel overwhelming. But by working together and finding common ground, we can overcome any obstacles that come our way.

3.2 Addressing the SWOT in future work of EMERALD

The EMERALD consortium will be addressing the initial SWOT analysis in the upcoming work package 6 deliverables on exploitation, D6.6 [1] and D6.7 [2]. We will be mapping the different findings to the initially identified stakeholders [3]. The key messages to be communicated to the various stakeholders have been defined in the EMERALD Communication Strategy (see D6.2 [5]), and include the following:

- Cloud Service Providers (CSPs): Emphasise the benefits of adopting a framework such as the one proposed by EMERALD to achieve ongoing certification. This includes demonstrating how the framework can improve the efficiency and effectiveness of certification processes by enabling continuous monitoring and assessment of security standards.
- ENISA/national agencies: Demonstrate the benefits of the continuous certification framework to achieve and maintain compliance with EU-wide cloud security certification standards. This includes discussing how the framework can help harmonise certification procedures and increase transparency for consumers.
- Auditors/accredited bodies: Emphasise how the EMERALD framework can strengthen the role of auditors and accredited bodies in verifying and confirming compliance with safety standards.
- Technical community: Emphasise the innovative nature of the EMERALD solution. This includes highlighting the technological advances and research that have gone into the development of the framework and the potential impact on improving cloud security.
- General public and cloud service users: Illustrate how a continuously certified cloud service provider ensures the security of data and services at different levels. This can be done by presenting case studies or examples that show how the framework works in practice and how it helps to protect consumers.

4 Analysis of Standardization Activities

Standardization plays a pivotal role in the success and effectiveness of the EMERALD project. The need for standardization arises from the diverse and evolving landscape of certification schemes in Europe, each with its unique set of metrics, values, and compliance requirements. By standardizing the metrics and values stored in the database, the project ensures compatibility and interoperability with multiple certification schemes, facilitating seamless data exchange and alignment with varied compliance standards. This standardization effort streamlines the certification process for cloud providers, enabling them to leverage EMERALD's information service consistently across different certification frameworks, leading to improved efficiency, accuracy, and reliability in compliance management and reporting.

Furthermore, standardizing various aspects of the certification process enhances the exploitation of the project results by establishing a unified and structured approach to data management, data exchange, and compliance assessment. Consistent data formats, metadata standards, and reporting templates ensure that compliance information stored in the database is accessible and understandable across certification schemes, promoting transparency and clarity in compliance reporting. Standardization also fosters interoperability, enabling seamless integration with existing certification systems and facilitating data sharing between cloud providers and certification bodies. By aligning with industry best practices and regulatory requirements through standardization, the EMERALD project enhances the trust, credibility, and usability of its information service, empowering cloud providers to achieve and maintain continuous certification with confidence and ease.

This section of the deliverable is informed by a combination of:

- A brief survey aimed to gain a comprehensive understanding of the current status of certification processes and to identify the needs for standardization among our pilot partners. This survey, which is attached in *APPENDIX B: Survey on Standardization Requirements*, serves as a crucial component in shaping the standardization activities required to ensure compatibility and interoperability with multiple European certification schemes. By engaging our pilot partners in this survey, we intended to gather valuable insights, perspectives, and suggestions that will inform our standardization efforts, enhance the effectiveness of our information service, and ultimately support cloud providers in achieving and maintaining continuous certification with efficiency and precision.
- Another inquiry was made by email to gather the current relationships of partners to standardization bodies.
- Online research done to obtain the above information from other entities, similar initiatives and industry practices.

The results of this activity provided valuable data for identifying common challenges, defining key requirements, and guiding our standardization strategies to align with the diverse needs and expectations of our pilot partners.

4.1 Processes related to Certification in Pilot Partners

The security controls management and assessment approach within our pilot partners' organizations is a hybrid model encompassing both automatically generated controls and manually produced evidence. They adhere to rigorous internal governance procedures, diligently connecting and aligning all evidence and relevant activities with a wide range of controls. Regular security audits, such as BSI C5, BSI 200-1, and ISO 27001, are conducted annually, complemented by internal security audits for thorough evaluation and monitoring of security measures.

Based on the input received from the pilot partners regarding achieving interoperability and integration within their companies, it is evident that interoperability between different certification schemes holds significant importance to them. To facilitate this, the partners emphasize the importance of an integrated security audit that is widely supported by their customer base.

The partners express their preference for a unified approach, leveraging an integrated security audit that aligns with industry standards. Specifically, they mention the utilization of Certification 200-1, an extension of ISO 27001, and C5, which is specifically tailored for cloud services. They highlight that there is a degree of shared documentation between Certification 200-1 and C5, allowing for synergies in documentation processes.

In order to enhance interoperability and integrate different certification schemes effectively, the partners mention their strategy of mapping these schemes to their internal control matrix. By aligning the requirements of ISO 27001 with the lean documentation approach it offers, they have been able to leverage some shared documentation elements across Certification 200-1 and C5. This approach not only streamlines their documentation processes but also facilitates greater compatibility and coherence between different certification schemes.

In terms of data handling and reporting measures within the pilot partner companies, the responses provided shed light on their operational practices. At CloudFerro, manual audits are conducted, resulting in comprehensive audit reports that emphasize observations and corrective actions. These findings serve as the basis for discussions and subsequent implementations within the company. On the other hand, Fabasoft leverages a document and workflow management Software as a Service (SaaS) solution within their ecosystem, enabling efficient management of documents and workflows to ensure operational compliance and seamless business processes.

The pilot providers emphasized the significance of enhanced value in standardized cybersecurity certifications. In their opinion, in recent years, the importance of certifications has somewhat diminished due to the proliferation of standards and certification bodies, allowing easier acquisition through financial means. Simplification and standardization of requirements are seen as key factors that can benefit companies such as CloudFerro by streamlining processes, reducing time and overhead costs. The harmonization of existing certification schemes, along with the support for available metrics and reference implementations for specific sets of requirements, is deemed essential in improving the overall security posture of cloud providers.

4.2 Identified Challenges

4.2.1 Related to Assessment of Security Controls

Ensuring the compatibility of metrics and values stored in the database with various European certification schemes is crucial for streamlining the security controls assessment process for cloud providers. To achieve this, the standardization requirements that need to be addressed include:

Defining a common data model and data format for storing security control assessment results. This standardized format should encompass all relevant metrics and values in a structured and easily accessible manner. By defining a common data model, it allows for consistent interpretation and comparison of security control assessments across different certification schemes, facilitating interoperability and efficient data exchange between various parties involved in the certification process.

Moreover, **establishing data normalization guidelines** is essential to ensure uniformity in data representation, enabling seamless integration of assessment results into different certification frameworks. By normalizing the data, it becomes easier to aggregate, analyse, and report on security control assessments, enhancing the overall transparency and reliability of compliance information stored in the database.

Furthermore, another critical standardization requirement is **the adoption of common terminology and definitions** for security controls and assessment criteria. By aligning the language used to describe security controls across different certification schemes, it reduces ambiguity and confusion during the assessment process. Standardizing terminologies ensures that cloud providers have a clear understanding of the security requirements and criteria specified by different certification bodies, enabling them to implement and assess security controls effectively. Additionally, establishing a unified set of definitions for assessment criteria promotes consistency in the evaluation of security controls, allowing for more accurate and reliable comparison of compliance status across different certification schemes. This harmonization of terminology not only simplifies the assessment process for cloud providers but also facilitates communication and collaboration among stakeholders involved in the continuous certification of cloud services.

4.2.2 Related to Aligning Certification Requirements

Several standardization initiatives and organizations address the security posture of cloud providers in Europe and play a significant role in the area of cybersecurity compliance. Table 6 shows the certifications offered by these agencies to the Pilot partners of EMERALD.

Table 6. EMERALD Pilot partners, Services and current Certifications

Partner	Services Involved	Years in Cloud Services	Certifications of Interest	Time for Sec. audit preparation
CloudFerro	IaaS, PaaS	9 years	ISO 27001, BSI 200-1, BSI C5	80 -130hrs
Fabasoft	SaaS	36 years	ISO 9001, ISO 20000-1, ISO 27001, ISO 27018, C5,	A continuous process
IONOS	IaaS	36 years	ISO 27001, ISO/IEC 27001, BSI C5,	A continuous process
CaixaBank	SaaS	5-6 years	ISO 27001, ISO 27017, ISO 22301	Continuous evaluation of the compliance status of their providers
OpenNebula	IaaS, PaaS	14 years	ISO27001	Not applicable

Based on the feedback gathered from the pilot providers regarding the challenges they encounter during audit preparations for multiple certification schemes, the following key points have been identified:

- **Document Updating Burden:** C5 and 200-1 certifications necessitate extensive document updates for audits, leading to time-consuming efforts. Many of these documents have limited relevance to daily operational activities and are primarily generated or revised solely for audit purposes. In contrast, ISO 27001 follows a more streamlined approach with minimal documentation requirements. For example, IONOS

is forced to maintain numerous excel files and thousands of Jira tickets to accomplish documentations in preparation for audits.

- **Certification Scheme Variation:** The diversity of certification schemes, such as CSA STAR, ISO 27017, and ISO 27018, poses challenges as customers inquire about various certification options. The aim is to minimize the number of certificates to the essential minimum, reflecting the complexity of managing multiple certification requirements. This was described by the pilot partners, as a time-consuming work. Specifically, they mentioned, finding the right measurement or metric for a requirement to produce evidence that suites the auditor’s interpretation of the requirement (Fabasoft) and when new type of certification is needed or in case a standard is updated, information from different departments or other audits need to be collected. Sometimes controls require implementation of a new process or preparation of documents (CloudFerro).
- **Audit Consolidation Difficulty:** The aggregation of audits for different certification schemes into a single cohesive process is challenging. Cloud Ferro mentioned that attempts to combine C5 and 200-1 audits to save time yielded limited efficiency gains, with certification bodies indicating minimal time-saving benefits from consolidating audits.
- **Limited Local Audit Resources:** In the case of CloudFerro, the unavailability of local companies (Polish) proficient in performing C5/200-1 audits resulted in reliance on German certification bodies. This geographical constraint impacts the audit process, highlighting the need for flexible audit resource availability.
- **Market-specific Certification Expectations:** Market preferences for certification schemes vary regionally, with German customers prioritizing BSI C5 or 200-1 certification, English market customers favouring Cyber Essentials, and other customers opting for ISO 27001. Aligning certification choices with customer expectations requires strategic planning to meet diverse market demands effectively.
- **Enhanced Multi-party Recognition Opportunities:** There is a desire to explore possibilities for leveraging multi-party recognition among certification schemes. Enhancing interoperability and recognition between different certification frameworks could streamline the certification process and enhance operational efficiency for cloud providers seeking compliance across various schemes.

Our wider industry research also confirms that diversity of the certification schemes in the cloud industry brings the challenges of repetitive work. The issue in this regard is that, in the European cybersecurity landscape, various certification schemes, such as ISO/IEC 27001, GDPR, ENISA certification schemes⁴⁷, PCI DSS, and CSA STAR Certification, pose significant challenges due to the lack of interoperability and standardization. These certification frameworks exhibit notable incompatibilities and differences in various aspects of the assessment process, creating obstacles for cloud providers seeking certification from multiple schemes. Below some examples of such incompatibilities.

- **In metrics and compliance requirements:** ISO/IEC 27001 emphasizes data encryption standards while GDPR focuses on privacy protection⁴⁸. Similarly, PCI DSS prioritizes access control policies, reflecting disparate priorities in the compliance assessments across different frameworks.
- **In data reporting formats:** Each certification scheme has its unique data reporting formats. For example, while GDPR requires detailed reporting on security incidents, CSA STAR Certification places more emphasis on compliance status summaries⁴⁹. These

⁴⁷ <https://www.enisa.europa.eu/news/enisa-news/cloud-certification-scheme>

⁴⁸ <https://www.iso.org/standard/27001>

⁴⁹ <https://gdpr-info.eu/>

differences can hinder data aggregation and comparison, impacting the efficiency of compliance reporting across multiple schemes.

- **In data security and privacy standards:** Certification schemes like ENISA certification schemes may stress encryption protocols, whereas PCI DSS may emphasize access controls⁵⁰. These disparities can complicate compliance efforts for cloud providers, especially when aligning with multiple certification frameworks.
- **In audit and assessment protocols:** The assessment methodologies of certification schemes vary extensively. For instance, PCI DSS may have different audit protocols compared to ISO/IEC 27001⁵¹. These differences can lead to disparate security assessments and compliance interpretations.
- **In cross-certification requirements:** Cross-certification requirements between schemes can also differ significantly. GDPR's requirements for recognizing certifications obtained from ENISA guidelines may differ, posing challenges for cloud providers seeking acknowledgment across frameworks⁵².

The divergent approaches of certification schemes highlight the pressing need for standardization and interoperability initiatives, such as EMERALD within European cybersecurity certification frameworks. Addressing these discrepancies can enhance the consistency, credibility, and effectiveness of cybersecurity certification processes for cloud providers. By addressing these challenges and considerations, the EMERALD project can develop a standardized approach that accommodates the diverse requirements of multiple European certification schemes, facilitating seamless interoperability and accessibility for cloud providers seeking continuous certification assurance.

4.2.3 Suggested by Pilot Partners

The pilot partners emphasised that the implementation and management of controls and metrics across various cloud service models present a significant challenge. Fabasoft and Cloud Ferro both shared their view that Standardizing cybersecurity certification processes has the potential to streamline audit preparation, reduce audit duration, and lower associated costs. Additionally, standardization could enhance automation, optimize processes, facilitate easier preparation work, and allow for the reuse of evidence when applicable. Ultimately, it would minimize the "switching costs" associated with changing audits or auditors, leading to increased efficiency and cost-effectiveness.

As cloud service users within the banking sector, CXB recognizes that standardization has the potential to streamline the evaluation of cloud services and mitigate subjectivity in defining and implementing controls and metrics.

Based on the feedback received from pilot providers regarding improvements they seek in the cyber security certification process, the following key points have been identified:

- Simplification of requirements to make the standards more concise.
- Development of an expanded repository containing standardized metrics.
- Global standardization efforts to decrease the number of differing standards worldwide.
- Restoration of customer trust in certifications, emphasizing their significance beyond mere purchasable documents.
- Enhanced support for multi-scheme certification through tools like the requirements mapping assistant.

⁵⁰ <https://www.enisa.europa.eu/topics/certification>

⁵¹ <https://www.pcisecuritystandards.org/>

⁵² <https://cloudsecurityalliance.org/blog/2023/11/03/csa-star-certifications-what-are-they>

- Increased value of standardized cybersecurity certifications to amplify their significance in the industry.

4.3 Opportunities Presented by Standardization Initiatives

The alignment of EMERALD with key standardization initiatives such as the European Cybersecurity Certification Scheme for Cloud Services (EUCS)⁵³ and the Open Security Controls Assessment Language (OSCAL)⁵⁴ presents invaluable opportunities for the project. By integrating with these initiatives, EMERALD can ensure compatibility with European certification requirements, enhance interoperability with various certification schemes, and ultimately improve the efficiency and credibility of our platform in the cloud service compliance landscape.

European Cybersecurity Certification Scheme for Cloud Services (EUCS)

EUCS, created by ENISA, aims to harmonize cybersecurity certification schemes across the European Union, providing a common framework for assessing and certifying the security of cloud services. By aligning EMERALD with EUCS, we can ensure that the metrics and values stored in our database are compatible with the requirements set forth by EUCS. This alignment will not only facilitate the certification process for cloud providers using EMERALD but also enhance the credibility and trust associated with our product within the European market, fostering wider acceptance and adoption.

AI Cybersecurity Initiatives

EMERALD can leverage the ongoing efforts of the AI Cybersecurity Working Group of ENISA⁵⁵ and the Criteria Catalogue for AI Cloud Services (AIC4) by BSI⁵⁶ to enhance its proof of concept. By aligning with the standards and criteria defined by these initiatives, EMERALD can showcase a solid foundation for ensuring the security and compliance of AI-based components. Adopting the guidelines and metrics provided by them will enable EMERALD to demonstrate its commitment to best practices in AI security and compliance. This strategic alignment can not only strengthen the project's technical capabilities but also position EMERALD as a reliable and forward-thinking solution for cloud providers in the evolving landscape of AI technologies.

Open Security Controls Assessment Language (OSCAL)

OSCAL is a government-driven (NIST) initiative focused on developing standardized formats and languages for expressing security and compliance information. Integrating OSCAL capabilities into EMERALD will enable us to utilize a common language for describing security controls and assessment results, making it easier to exchange information with different certification schemes. By adopting OSCAL, EMERALD can efficiently communicate security-related data, ensuring consistency and coherence across various compliance frameworks. This alignment with OSCAL will streamline the auditing and certification process for cloud providers, ultimately enhancing the reputation and marketability of EMERALD. The EUROSCAL⁵⁷ initiative kickstarted

⁵³ <https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme>

⁵⁴ <https://pages.nist.gov/OSCAL/>

⁵⁵ https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/artificial_intelligence/ad-hoc-working-group

⁵⁶ https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/AIC4/aic4_node.html

⁵⁷ <https://euroscal.eu/>

by the MEDINA⁵⁸ project in June 2023 can play an important role in further driving this objective with EMERALD.

By actively engaging with standardization initiatives such as EUCS and OSCAL, EMERALD can position itself as a reliable and interoperable solution for cloud providers seeking continuous certification in the European market. The compatibility with these initiatives will not only simplify the compliance process but also bolster EMERALD's reputation as a trusted platform for managing and demonstrating compliance with multiple certification schemes.

4.4 Collaboration with Standardization bodies

In order to drive the EMERALD project towards successful standardization and interoperability with various European certification schemes, a second inquiry was made among our project partners to assess their current relationships with standardization bodies. The purpose of this inquiry was to gather key insights on the partners' levels of engagement, membership status, and participation in standardization-related events. This information is crucial for designing a strategic standardization roadmap for the EMERALD project, ensuring that the project will align seamlessly with the requirements of multiple certification schemes. Table 7 shows a summary outlining the status of the relationships our partners have with standardization bodies.

Table 7. Current Engagement in Standardization bodies

Partner	Standardization group	Participation
TECNALIA	ISO/IEC CTN 320 "Cybersecurity and Data Protection"	Member
	ISO/IEC CTN 320/SC 01 "Cybersecurity Management Systems"	Member
	ISO/IEC CTN 320/SC 05 "Data Protection, Privacy and Identity Management"	Member
	ISO/IEC CTN 071/SC 307 "Blockchain and Distributed Ledger Technologies"	Member
	Gaia-X	Member
Fraunhofer	Gaia-X	Member
FABA	ETSI - TC-CYBER and TC-SAI	Member
	ASI (Austrian Standards International)	In Contact
	CEN-CENELEC	In Contact
	Gaia-X	Member
SCCH	ASI (Austrian Standards International)	Member
	AI Advisory Board of the Austrian Federal Government	Member
	EurAI (European Association for Artificial Intelligence)	Member
	TÜV (Technischer Überwachungsverein)	In Contact
KNOW	BDVA (Big Data Value Association)	Member
	Digital Innovation Hubs	Member
	Platform Industry 4.0: Data Spaces	Member
	Gaia-X	Member
IONOS	Gaia-X	Member

To summarise this section, standardization plays a pivotal role in the success and ultimate exploitation of the EMERALD project results. Through the comprehensive analysis of requirements outlined in this section, supported by valuable insights from pilot partners and

⁵⁸ <https://medina-project.eu/>

extensive online research, it is evident that establishing compatibility and interoperability of data and process are essential for seamless integration with various European certification schemes. By adhering to robust standardization practices, EMERALD ensures that the evidence management service developed for continuous certification in the cloud can be leveraged effectively by cloud providers, facilitating streamlined auditing processes and enhancing overall compliance management. Embracing standardization not only fosters trust and credibility but also paves the way for broader adoption and utilization of the project outcomes, thereby maximizing the impact and value proposition of EMERALD in the realm of cloud service certification.

DRAFT

5 Conclusion

Conducting a thorough market analysis is a crucial preliminary step to establishing a business. It serves to ascertain pertinent information about the target market and assess potential risks. It is important to note that market analysis is inherently reliant on estimations, as even the most comprehensive statistics may not offer definitive answers to specific product-related inquiries. Nevertheless, the more detailed and precise the research, the more accurate the forecasts will be, thereby enhancing the likelihood of a successful venture.

As a founder, it is crucial to anticipate future market developments. A market potential analysis should address concerns such as potential labour requirements, barriers to market entry (e.g., costs), key success factors and upcoming market trends. Investors will be particularly interested in the results of this market potential analysis.

Analysing market potential is a comprehensive process that involves a thorough assessment of market size, growth potential, competitive landscape and customer needs. It is important to collect both quantitative and qualitative data to enable a well-founded assessment of market opportunities and risks. This can be done through a combination of secondary research, such as analysing industry reports and market data, and primary research, such as surveys and interviews with potential customers and industry experts.

The key messages to be communicated to various stakeholders include:

- Cloud Service Providers (CSPs): We will highlight the benefits of adopting a framework like the one proposed by EMERALD for achieving ongoing certification.
- ENISA/national agencies: We will showcase the advantages of the continuous certification framework for obtaining and maintaining compliance with the EU-wide cloud security certification standards.
- Auditors/ accredited bodies and technical community: We will emphasize the innovative nature of the EMERALD solution.
- General Public and cloud service consumers: We will illustrate how a continuously certified CSP ensures the security of data and services at different levels.

Communicating these messages requires a clear and coherent strategy that ensures that each stakeholder group receives the information that is most relevant to them. This can be achieved through targeted marketing and communication campaigns, educational workshops and partnerships with industry associations and regulators.

The standardization efforts within the EMERALD project are pivotal for ensuring compatibility and interoperability with diverse European certification schemes, and drive exploitation of the outcomes. By establishing a unified approach to data management and compliance assessment, standardization streamlines the certification process for cloud providers, enhancing efficiency, accuracy, and reliability in compliance management and reporting. Identified challenges such as compatibility issues, documentation burden for audits, and certification scheme variations underscore the need for standardized processes. The integration with key initiatives like EUCS and OSCAL presents opportunities for aligning with European requirements, enhancing credibility, and promoting interoperability. Collaboration with standardization bodies and addressing suggested improvements by pilot partners will be crucial for implementing standardized cybersecurity certification processes, optimizing processes, and streamlining audit preparation efforts. Through these initiatives, EMERALD aims to maximize its impact and value proposition in the domain of cloud service certification.

The future actions for the EMERALD project include developing and implementing a common data model and format for storing security control assessment results, establishing data

normalization guidelines, and aligning terminology and definitions for security controls and assessment criteria. The project will address challenges by streamlining documentation processes, standardizing certification scheme variations, and improving audit consolidation efficiency to enhance interoperability and integration across certification schemes. Collaboration with standardization bodies and key initiatives like EUCS and OSCAL will be prioritized to ensure compatibility and credibility. Implementing pilot partners' suggestions to optimize audit preparation, reduce duration, and increase automation in cybersecurity certification processes will drive efficiency and cost-effectiveness. These actions aim to reinforce EMERALD's role as a trusted and efficient solution for continuous certification in the cloud industry. These future actions will be measured against KPI 9.2, encompassing the development of a Standardization roadmap, providing guidance on interoperability with OSCAL, and contributing a set of metrics to EUCS, ETSI, ENISA, CIS, NIST, and BSI.

Continuous certification of cloud services is an important step towards a more secure and trustworthy cloud environment. By implementing a framework such as EMERALD, cloud service providers can demonstrate their commitment to maintaining the highest security standards and increase customer and investor confidence. For the technical community, it provides a platform for innovation and collaboration, while for the general public and users of cloud services, it provides an additional layer of security.

References

- [1] EMERALD Consortium, “D6.6 Exploitation Report - v1,” 2025.
- [2] EMERALD Consortium, “D6.7 Exploitation Report - v2,” 2026.
- [3] EMERALD Consortium, “EMERALD DoA,” 2022.
- [4] MEDINA Consortium, “MEDINA D5.5 Integrated Solution v3,” 2023.
- [5] EMERALD Consortium, “D6.2 Dissemination and Communication strategy,” 2024.

APPENDIX A: Links of additional competition findings

The following links contain possible competition for future reference and future market research:

- Zscaler Zero Trust Exchange - <https://www.zscaler.com/resources/data-sheets/zscaler-cspm-free-trial-datasheet.pdf> Leader in the 2023 Gartner Magic Quadrant for Security Service Edge (SSE)
- Prisma Cloud PaloAltoNetworks - <https://www.paloaltonetworks.es/prisma/cloud>
- ForcePoint - <https://www.forcepoint.com/>
- Netskope - <https://www.netskope.com/>
- WIZ Cloud Security Platform - <https://www.wiz.io/>
- IBM Security - <https://www.ibm.com/security>
- Tenable - <https://www.tenable.com/>
- Coalfire - <https://www.coalfire.com/>
- AWS Cloud Compliance - <https://aws.amazon.com/en/audit-manager/>
<https://aws.amazon.com/en/cloudops/compliance-and-auditing/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc&blog-posts-cards.sort-by=item.additionalFields.createdDate&blog-posts-cards.sort-order=desc>
- Google Cloud Audit Logs - <https://cloud.google.com/audit-logs?hl=en>
- Aqua - <https://www.aquasec.com/products/cspm/>
- ScoutSuite - <https://github.com/nccgroup/ScoutSuite>
- CloudSecuritySuite – <https://github.com/SecurityFTW/cs-suite>
- Prowler - <https://github.com/toniblyx/prowler>
- Intruder - <https://www.intruder.io/>
- Datadog - <https://www.datadoghq.com/product/cloud-security-management/>
- Sonrai Security - <https://sonraisecurity.com/>

APPENDIX B: Survey on Standardization Requirements

This section presents the content of the survey that has been completed by the pilot owners. The objective was to gain an in-depth understanding of the current status of their certification processes and to identify their standardization needs.



EMERALD

Evidence Management for Continuous Certification as a Service in the Cloud

Survey on Standardization Requirements of Cybersecurity Assessment and Certification Processes for Cloud Service Providers

The following survey aims to gather insights on the standardization requirements of the cybersecurity certification processes of cloud services from the Pilot partners of EMERALD. Feedback obtained is crucial and only to be used for further development of EMERALD towards enhancing interoperability and compliance across certification schemes.

Dear EMERALD Partner, please provide your valuable input by responding to the following open questions. Feel free to include any additional information that you see as relevant.

1. General Information:
 - Name of your organization:
 - Type of cloud services offered (e.g. PaaS, SaaS, IaaS, hybrid, etc.):
 - Number of years your organization has been in the cloud services industry:
 - Types of Certifications you have obtained/applied for/plan to apply for:
 - In average how long does it take your company to prepare documentation for security audits?
2. Security Controls Assessment:
 - a. How do you manage and perform assessments of security controls within your cloud services?
 - b. Are you facing challenges with aligning the use and performance of security controls with requirements of different certification schemes? If yes, please elaborate.
3. Standardization Needs:
 - a. Do you believe standardization of cybersecurity certification processes, metrics etc. would benefit your organization? Why or why not?
 - b. What specific areas of the process do you find most challenging to standardize across different cloud service models (PaaS, SaaS, IaaS) and certification schemes?
4. Compliance and Certification Process:
 - a. How do you currently handle certification and compliance processes across multiple schemes?

- b. What key challenges does your company encounter when aligning your security controls with certification requirements and metrics?
5. Interoperability and Integration:
 - a. How important is interoperability between different certification schemes for your company?
 - b. What measures does your company currently take to ensure interoperability and data exchange with various certification systems?
6. Data Handling and Reporting:
 - a. How does your company manage and store compliance status information for auditing purposes?
 - b. Are there specific data formats or reporting templates you find challenging when dealing with multiple certification schemes?
7. Improvement Suggestions:
 - a. What improvements or standardization initiatives would you like to see in the assessment for and data management of cybersecurity certification of cloud services?
 - b. How do you believe standardized cybersecurity certification can enhance the security posture and compliance of cloud service providers?
8. Future Considerations:
 - a. In your opinion, what are the key factors that should be considered in the standardization of cybersecurity certification of cloud computing services?
 - b. How can standardization efforts further support the interoperability and efficiency of compliance processes for cloud service providers?
9. Any other comments: