

Core Business Systems Cloud Strategy

A Hybrid Multi-Cloud Hosting Framework Public Edition

April 2025

Contents

Contents	2
1. Introduction	3
1.1. Glossary	3
2. Current context and drivers	5
2.1. Mission and vision.....	5
2.2. eu-LISA baseline: Current state.....	5
2.3. Contextual/environmental analysis	6
3. Strategic goals for 2021-2027	8
4. Related documents	10

© eu-LISA, 2025

This document is public.

Reproduction is authorised, except for commercial purposes, provided that the source is acknowledged.

1. Introduction

The Agency is tasked with the development and operational management of large-scale IT systems in the Justice and Home Affairs area. The Agency is committed to employing technologies that offer optimal cost-benefit ratios for its Core Business Systems (CBS) and additional components that it is entrusted with, in alignment with its own mandate and operational requirements.

The Agency is currently overseeing a significant expansion of new Core Business Systems, including EES, ETIAS, IO, ECRIS-TCN, eCODEX, JIT, eVISA and emerging proposals for PRUM and API. This extension necessitates substantial IT infrastructure installations at the Agency's technical sites: the Central Unit (CU) in Strasbourg, France, and the Backup Central Unit (BCU) in Sankt Johann, Austria. These facilities are now operating at maximum capacity in terms of available power, cooling and space.

Over the past decade, the IT industry has seen the rise of cloud technologies because they offer better value for money, are more scalable, and in some cases are more reliable than providing those IT services on-premise. Additionally, the available human resources for development and maintenance are limited within the Agency, and using managed platform and software services could address some of these concerns. These cloud technologies offer potential solutions for offloading the Data Centres in the Agency's technical sites and dedicating their capacity for CBS environments or CBS data the Agency has to have on-premise to comply with its regulatory framework. The proposed strategy is designed to complement and enhance the Agency's future sourcing strategy, providing a framework for making informed decisions about infrastructure investments and service procurement.

In response to these evolving demands and opportunities, this document describes the Agency CBS Cloud Strategy: A Hybrid Multi-Cloud Hosting Framework. This strategy aims to streamline the IT infrastructure provision through a hybrid approach, balancing on-premise and cloud hosting solutions. The objectives are to accelerate system development and time-to-market, optimize IT resource management, ensure continued compliance with relevant regulations, and maintain robust security measures.

This strategic initiative represents a pivotal step in transforming the Agency's IT infrastructure, enhancing its development capabilities and operational efficiency. By embracing a hybrid model, the Agency positions itself to meet current challenges while preparing for future demands in the dynamic landscape of European justice and home affairs IT systems.

1.1. Glossary

For the purpose of this strategy, the mentioned terms throughout this document have the following meaning:

Name	Acronym	Description
Core Business System	CBS	An IT Information system governed by a legal basis and entrusted to the Agency for development and/or operations. Examples include the SIS, VIS, EURODAC, EES, ETIAS, IO, ECRIS-TCN, JIT information systems.
Central Unit	CU	eu-LISA technical site located in Strasbourg, France

Backup Central Unit	BCU	eu-LISA business continuity site located in Sankt Johann im Pongau, Austria.
Infrastructure as a Service	IaaS	A computing model where a third-party provider hosts and maintains core infrastructure components such as servers, storage, and networking resources. Users can access and manage these resources, allowing them to build and run their own platforms and applications without the need to maintain physical hardware.
Platform as a Service	PaaS	A computing model that provides customers with a complete development and deployment environment. PaaS includes infrastructure (like IaaS) but also middleware, development tools, database management systems, and more. This allows users to develop, run, and manage applications without the complexity of maintaining the underlying infrastructure.
Common Shared Platform	CSP	Scalable, agile, and standardised on-premise platform, offering a resource-efficient framework and streamlined development and operational platform using PaaS model
Comprehensive Cloud Platform	CCP	Scalable, agile and secure cloud platform, based on Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS), offering faster setup and easier scaling of application environments

2. Current context and drivers

2.1. Mission and vision

*The **eu-LISA core mission** is to support through technology the efforts of the EU and its Member States to keep Europe open and secure*

*The **Agency vision** targets to continue providing high-quality efficient services and solutions, systematically aligning the capabilities of technology with the evolving needs of the EU and the Member States, maturing as a recognised and trusted partner in driving the digital transformation in the Justice and Home Affairs domain.*

In order to support the fulfilment of this mission (and to achieve the vision), the Platform and Infrastructure Unit in the Agency aims to:

- Implement a flexible and scalable infrastructure provisioning model that optimizes the balance between cost efficiency, performance, and security, tailored to the various workloads and data types.
- Enhance operational efficiency through automation and streamlined maintenance processes, reducing manual workload and improving the management of system updates and patches
- Accelerate the delivery of new systems and updates to existing systems by adopting agile infrastructure provisioning methods that enable faster deployment and parallel development and testing processes.
- Adhere to the strict security and data protection rules imposed on by the agency, by using state of the art technology principles, tools and processes.

2.2. eu-LISA baseline: Current state

eu-LISA's infrastructure landscape has undergone significant evolution since its establishment in 2012. Initially, the agency inherited a completely siloed IT infrastructure for each system (SIS, VIS, EURODAC), with separate on-premise infrastructures for production, pre-production, and test environments. In 2017, eu-LISA introduced the Common Shared Infrastructure (CSI) model, aiming to mutualize certain IT resources and management services while maintaining largely dedicated compute resources for each system. This approach was applied to the EES and sBMS components. More recently, in 2023, the Smart Hosting initiative was launched, comprising of the Common Shared Platform (CSP) and the Comprehensive Cloud Platform (CCP). The CSP further mutualizes infrastructure resources, creating a unified platform for systems such as ETIAS, ECRIS-TCN, and IO. These applications rely on common platform services, enabling also the interoperability agenda as outlined by the Agency. Additionally, the CCP has been utilized to provide infrastructure services to the e-CODEX application, demonstrating the smart hosting versatility in supporting various systems.

Despite these advancements, the Agency now faces critical challenges that necessitate a new strategic approach. The massive growth in the number of CBS to be developed, and this with a production, pre-production and test environments imposes large investments and capacity enhancements. The technical sites in CU and BCU are approaching their physical limits in terms of electricity, cooling, and space. This restrains the Agency's ability to expand and accommodate new systems in the future in BCU. Furthermore, the growing number of systems is placing increased strain on the operational staff and the operational budget.

The current infrastructure model, primarily reliant on on-premise data centres, has some limitations to meet the evolving demands of EU's Justice and Home Affairs domain. The historical contracting and waterfall development approach results in extended lead times for provisioning new infrastructure, causing delays in the deployment of new systems and the evolution of existing ones.

Implementing a cloud strategy is crucial for eu-LISA to overcome these challenges. Such a strategy is addressing the physical limitations of current data centres, optimize and fine tune infrastructure utilization, enhance operational efficiency, and accelerate system deployment. It should also ensure scalability for future growth while maintaining the levels of security and compliance required by the applicable legal frameworks.

2.3. Contextual/environmental analysis

To provide context for the current challenges, it's important to note the sudden influx of new systems that the Agency has been tasked with developing and managing. Significantly, no new Data Centre facilities have been foreseen in the Legal Financial Statements (LFS) that accompany the Regulations of these new systems (EES, ETIAS, IO, ECRIS-TCN, JIT). Moreover, a proposed second Data Centre extension was not approved. These factors have contributed to the current capacity constraints and the need for a new strategic approach.

To address the aforementioned challenges, this strategy proposes a strategic move towards a hybrid multi-cloud hosting approach. This consideration is informed by two key analyses:

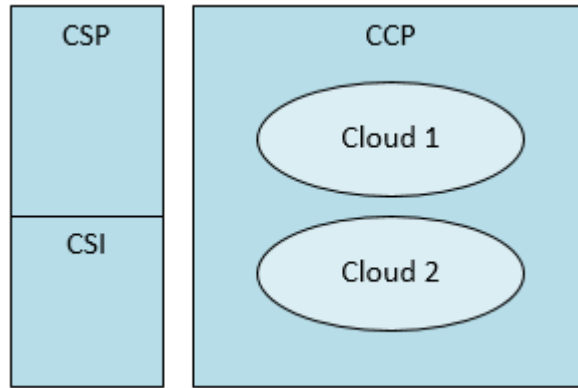
- Firstly, a legal analysis of which systems can be moved to the cloud, taking into account the strict regulatory framework within which eu-LISA operates .
- Secondly, a comprehensive investigation into whether eu-LISA can consider a move to the cloud and under what conditions. This analysis examines the technical feasibility, potential benefits, and operational implications of cloud adoption for the Agency.

Before detailing the proposed solution, it's important to note that several options were carefully considered. The primary alternative explored was a “cloud first strategy”, which would involve moving entire applications in the cloud, including production environments. This approach was thoroughly evaluated to fully leverage cloud benefits across all CBS and environments. However, this cloud first strategy was ultimately discarded as it would not align with the legal requirements that oblige the agency to maintain certain core production components on site..

After careful consideration of these legal constraints and operational needs, the proposed hybrid multi-cloud hosting approach emerged as the most suitable strategy for the Agency. The proposed hybrid multi-cloud hosting approach involves leveraging the Agency's existing infrastructure and enhance it capabilities. As illustrated in Figure 2, this strategy comprises three key components;

1. Common Shared Infrastructure (CSI): Provides on-premise Infrastructure-as-a-Service (IaaS)
2. Common Shared Platform (CSP): Builds upon CSI to offer on-premise Platform-as-a-Service (PaaS).
3. Comprehensive Cloud Platform (CCP): Extends capabilities to the public cloud, providing both IaaS and PaaS through at least two proven, strategic cloud platforms (Cloud 1 and Cloud 2).

PUBLIC



▲ Figure 1 the Agency's Hybrid Multi-Cloud Architecture - CSI, CSP and CCP components

This strategy would allow the Agency to leverage the benefits of cloud computing while maintaining compliance with strict regulatory and security requirements.

The legal analysis indicates that while production environments containing personal data must remain on-premises due to current regulations and geopolitical considerations, there is potential for moving non-production environments to the cloud. Furthermore, it suggests that even for production systems, non-core components that do not contain any personal data originating from the CBS could potentially be moved to the cloud, subject to further legal, security and data protection analysis and approval within the governance of the respective Core Business system (Advisory Group, Project Management Board, Management Board).

This nuanced approach would provide immediate benefits in terms of scalability, cost efficiency, and operational agility for non-production environments, while also opening up possibilities for future optimization of production systems.

A hybrid multi-cloud strategy would enable eu-LISA to:

1. Optimize infrastructure utilization and costs by leveraging the elasticity and pay-as-you-go models of cloud platforms.
2. Increase operational efficiency through automation and managed services, reducing the burden on eu-LISA's limited IT staff.
3. Improve agility and reduce time-to-market for new systems and updates by utilizing cloud-native development and deployment practices.
4. Enhance scalability and elasticity to meet changing demands, particularly for non-production environments used in development and testing.
5. Leverage advanced security capabilities provided by cloud platforms to augment eu-LISA's existing security measures.

3. Strategic goals for 2021-2027

This section analyses eu-LISA's strategic goals from the 2021-2027 long-term strategy, focusing on the CBS Cloud Strategy. A goal alignment methodology has been used to ensure the CBS Hosting objectives support eu-LISA's overarching strategic goals.

To illustrate this alignment:

- Table 2 illustrates the connection between eu-LISA's strategic goals for 2021-2027 and the specific goals of the CBS Cloud strategy. This alignment ensures that the functional strategy contributes directly to the agency's broader mission, particularly supporting Strategic Goal 1 (SG1), which focuses on eu-LISA's growth as an implementing partner in the Justice and Home Affairs domain.
- Building on this alignment, Table 3 provides an overview of the specific CBS Hosting goals, presenting both the current situation and expected achievements by 2027. This table serves as a roadmap for eu-LISA's CBS Cloud strategy implementation, covering key areas such as cloud migration, infrastructure as code implementation, cloud financial operations, and platform architecture standardization. For each goal, the current state and desired future state are articulated, offering a clear vision of the progress eu-LISA aims to achieve by 2027.

To guide this transformation, the Agency's infrastructure and platform framework is grounded in the '5S' general principles, which underpin the development and maintenance of transversal platforms hosting CBS applications within the Agency:

1. **Scalability:** With the Agency facing growing systems and workloads, we acknowledge the need for infrastructures that can effectively handle this expansion without any compromise on performance. We aim to implement solutions that can grow alongside our technological landscape, accommodating future needs seamlessly.
2. **Sustainability:** In response to a rapidly advancing technological landscape, we commit to staying up-to-date with stable supported hardware and software versions, integrating iterative practices, and continuously updating our systems to align with industry standards, security measures, and evolving technologies. This approach aims to optimise hosting solutions to be sustainable for the Agency in terms of needed resources.
3. **Stability:** Recognizing that the stability of our services is crucial to maintain trust and deliver efficient services to end-users, we have set our goal to achieve a 99.99% availability rate for production platforms, ensuring minimal downtime and seamless operations. Portability of the applications over the different platforms and consistency between the production and preproduction platforms needs to ensure reliable testing improving overall stability of the applications.
4. **Security and data protection:** Given that safeguarding of data is paramount. We commit to implementing robust security measures (e.g., security and privacy by design, encryption, access controls, proactive security monitoring, and security incident response) as requested by the applicable regulatory framework (namely, EU Regulation 2022/0085, Regulation (EU) 2018/1725) and best practises (namely, NIST Zero Trust, ISO 27001:2022, 27017:2015) maintaining the trust of stakeholders. With specific regard to data protection considerations, any processing of personal data shall comply with Regulation (EU) 2018/1725. The data managed in the off-premise cloud solutions must be devoid of any personal data originating from the core business systems. The only exceptions pertain to personal data necessary for granting access to agency staff or contractors tasked with development and maintenance of cloud solutions. Personal data linked to supporting tools needed for the development and maintenance of CBS (e.g. ticketing tool for incident management.) can also be stored off-premise.

5. Stewardship: To ensure long-term viability and avoid vendor lock-in, we will maintain control over critical components by leveraging trusted industry hardware, software and cloud vendors, and implementing vendor supported architectures and standards. We will promote platform standardization across all applications, ensuring they follow similar standards and architectures. This approach ensures data privacy and sovereignty, legal compliance, and independence in our decision-making processes. Cloud Providers must be able to ensure that the Agency's data remains at rest and in transit in the territory of the European Economic Area.

These principles are reflected in the specific goals outlined in Table 3, which provides a comprehensive overview of the current situation and expected achievements for each area of improvement.

eu-LISA Strategy 2021-2027	
eu-LISA strategic goals	Specific CBS Hosting objectives of the functional strategy
SG1: Continue to grow as an implementing partner and contributor to the relevant policies in the domain of Justice and Home Affairs.	Deliver and maintain highly secure, cost effective and continuously available platforms and infrastructure to the Core Business Systems entrusted to eu-LISA

Table 2. Connection between strategic goals for 2021-2027 and specific goals of the CBS Cloud strategy.

Specific CBS Hosting goals	Current situation overview	Expected achievements by 2027
1. Scalability: Enhance infrastructure provisioning	Infrastructure deployment largely manual, often time-consuming. Capacity increases lengthy procurement.	Significantly reduced lead time for infrastructure and platform provisioning By use of modern technologies and automation allocate resources in a dynamic way based on actual need
2. Sustainability: Optimise infrastructure footprint and cost	All infrastructure installed in on-premise locations (CU, BCU). Additional capacity requires modular DCs. The current financial framework does not have activity-based costing or "pay as you go models" to optimise the cost.	More efficient use of limited on-premise capacity within the Agency's Data Centres Increased capacity and scalability using secure cloud technologies where appropriate Implement a financial framework with FinOps capabilities for greater visibility and optimization of IT resource consumption
3. Stability: Improve operating model	The current operating model does not take cloud use into account.	Improved operating model in place with clear roles and responsibilities for involved units at each phase of the platform development and operations.
4. Security and Data protection: Implement robust security measures and compliance frameworks	Compliance, data protection, and security frameworks are mainly focused around on-premise hosting.	Ensure security, data protection, and legal frameworks are updated to take cloud environments into account, maintaining robust measures across all platforms.
5. Stewardship: Standardize platform architectures	No standardized 'blueprint' approach available	Deployed standardised platforms using pre-approved architecture patterns, leading to faster solution delivery and reduced cost of operations

Table 3. Overview of the current and desired state per each specific goal.

4. Related documents

- Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011
- Regulation (EU) 2023/2841 of the of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union;
- Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC;
- Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726
- Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011.
- Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226.
- Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast).
- Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA
- Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816
- Regulation (EU) 2023/969 of the European Parliament and of the Council of 10 May 2023 establishing a collaboration platform to support the functioning of joint investigation teams and amending Regulation (EU) 2018/1726

- Regulation (EU) 2024/982 of the European Parliament and of the Council of 13 March 2024 on the automated search and exchange of data for police cooperation, and amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, (EU) No 2019/817 and (EU) 2019/818 of the European Parliament and of the Council (the Prüm II Regulation)
- Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006
- Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU
- Regulation (EC) No 767/2008 of 9 July 2008 concerning the VIS and the exchange of data between Member States on short-stay visas (VIS Regulation)
- Regulation (EU) 2021/1334 of 7 July 2021 for the purpose of reforming the VIS (Implementing VIS Regulation)