# Digital Sovereignty

## Security and privacy

EXAM fall 2025


| Name | Initials | student number |
|---|---|---|
| Alexander Nygaard Thomsen | AT | 201911329 |
| **Lecturer: Christian Damsgaard Jensen** | | |


Due date: 11/12/2025

# Contents

**1 Executive Summary** **3**
1.1 overall conclusion . . . 3

**2 Introduction** **4**
2.1 Abbreviations . . . 4

**3 Current Technology and Service Landscape** **5**
3.1 Mediscan technology landscape . . . 5
3.2 HealthSync Mobile's technology landscape . . . 5
3.3 The hybrid environment post merger . . . 5
3.4 Identity and Access management . . . 6

**4 Dependency Analysis** **7**
4.1 Purpose . . . 7
4.2 Dependency mapping . . . 7
4.2.1 A. Cloud infrastructre Dependencies . . . 7
4.2.2 B. Identity & Access management Dependencies . . . 7
4.2.3 C. Application & SaaS Dependencies . . . 7
4.2.4 D. Security & Monitoring Dependencies . . . 7
4.2.5 E. Data processing & Clinical workflow Dependencies . . . 7
4.2.6 F. Development and Tooling Dependencies . . . 8
4.3 Current providers and dependency severity . . . 8

**5 Risk Assessment** **9**
5.1 Physical Vulnerabilities . . . 9
5.1.1 Viby site . . . 9
5.1.2 Lystrup site . . . 10
5.2 How Identified Risks Impacts LHT's Digital Soverignty . . . 11

**6 EU-Alternatives** **11**

**7 Comparison of current and proposed solution** **11**

**8 recommended migration strategy** **11**

**9 conclusion** **11**

# 1 Executive Summary

The purpose of this report is the examine, expand and define the organizations current dependancy on non-EU technology, evaluate the key risks associated with this direction, analyse and propose EU alternatives. The goal is to identify and map a road to digital Sovereignty.

The current political climate is quite inhospitable and it has become apparent that world leaders make drastic, snap decisions that brings large implication to the technological landscape, where big tech can be leveraged as political thus inherently changing the risk of reliance on such servies. Thus companies, with suchs reliances, risks getting caught in the crossfire.

Services where there is a heavy reliance, from companies such a *Microsoft*, which hosts Azure Active directory (AD), used for identity management and *SharePoint* and *OneDrive*, which Lifeline Health Technologies(LHT) uses as a file sharing service, could suddenly become unavailable.

A loss of this service, which would be tantamount to loss of many years of technological IPs and achievements which could lead to unquantifiable damage to the company. Thus, in this inclimate weather, a EU alternative for these servises, is quintessential.

The main findings of this report is an overreliance on

- Microsoft Azure Services, where cloud hosting is indeterminate and jurisdictional expose is somewhat vague. Thus EU laws may be hard to apply
- process and regulatory mismatches - Data is easily given up to 3rd party cloud services without regard for compliance (EU MDR)
- A thorough documentation is needed of other cloud solutions, specifically regarding SaaS tools
- main risks

Examples for some EU-alternatives :

- Univention - German based software for identity & access management. A self hosted AD, requiring a virtual machine. Can then handle all authentication, along with other features such as single sign-on(SSO) and multifactor authentication (MFA)
- Scaleway - A cloud hosting service, to host VM's for infrastructre purposes.

Thus Univention can be hosted by Scaleway, thus removing the dependancy on a Microsoft service.
In addition, the company's productivity suite, can be replaced by libre-office

## 1.1 overall conclusion

# 2 Introduction

This report addresses the current and ongoing challenges that is present within Lifeline Health Technologies ApS due to the merger between Mediscan ApS, an established manufacturor of ultrasound electronics equipment for the health industry. And HealthSync Mobile ApS (HSM), a younger, digital health oriented company. The two former companies originates from two different times, with differing missions and complex implementatitons.

The complexity created by thtis merger and associated difficulties, due to differing it-landscapes, has prompted the executive team, to commission this report to highlight, identify and analyse the requirements and dependencies, related to digital Sovereignty with a focus on non-EU providers. The purpose of this report therefore becomes to identify risks within the newly formed, yet disjointed, It invironment which LHT has inherited, with its included assets, and how dependencies has could cause problems regarding regulatory compliance, operation stability and long-term autonomy from non-EU actors.

The scope of this report covers the broader themes of digital Sovereignty, including identity and access management, data-storage, infrastructre and process mismatches, aswell as the risk associated with a futrure migration along with a focus on jurisdictional factors that arises when handling sensitive data or other regulated information.

The overall structure of this report is, an overview of the current technology and service landscape of LHT, and a accompanying dependancy analysis. These two tie into the risk assessment of the current status. This is followed by an evaluation of possible EU-alternatives to implemented services and comparison of the current implementatitoon. Lastly a recommended migration Strategy is proposed.

## 2.1 Abbreviations

| **Abbreviation** | **Meaning** |
|---|---|
| | |
| | |
| AD | Active Active directory |
| MFA | multifactor authentication |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

Table 1: Table of common abbreviations, used in this report

# 3 Current Technology and Service Landscape

As a result of the merger between Mediscan Aps and HealthSync Mobile Aps, the it environment, inherited to LHT, is comprised to two very different digital landscapes. These difference goes beyond mere technocal platforms, such as tool chosen for various tasks, but also divering filosophies. This leaves LHT to operation in a Hybrid environment, where some parts of the company use incompatible identity systems, inconsistent governance practices and service providers that might not be a perfect fit for EU regulations.

## 3.1 Mediscan technology landscape

Mediscan originates from traditional engineering practies, around product development, production, calibration and quality asurance. These include

- On-prem EU-local infrastructre, there the whole it system is segmented into various sub networks, for engineering, manufacturing and servers.
- Local AD controllers, running on older operating systems, with weak overall governance
- Weak network security regarding hardware, older switches with no updates
- No MFA and relying on password update rotations

The infrastructre inherited from Mediscan, shows strong prefence to local storage and authentication along with a typical product first approach, where cynersecurity is seen as a hinderance.

## 3.2 HealthSync Mobile's technology landscape

HSM oprates a rather modern techonology environment, based in the new cloud computing era. With a heavy reliance on popular service providers such as the Microsoft Azure suite, Google cloud and other Saas products. These include:

- An extensize implementation of Azure services such as: AD, kubernetes, Cosmos DB, PostgreSQL, Key Vault, Api management, blob storage and monitor + application insights.
- Heavy reliance on CI/CD pipelines and API updates, from non-EU cloud hosted services.
- JSON/WIRE-formatted data.
- Enforced MFA, and OAtuh2 + OpenID for access to apps

HSM's modern Technology stack, which histroically has granted them the capability for rapid expansion and growth comes at the cost of strong ties to non-EU governed cloud services. Which could become subject to outside EU regulation.

## 3.3 The hybrid environment post merger

The post-merger leaves LHT with a partially integrated and partially improved hybrid network, currently consisting of:

- The legacy on-prem VLAN of Mediscan's solution for manufacturing and engineering
- HSM's Azure environment and dependencies
- Site-to-site VPN between the two company environments

Inconsistent and overlapping infrastructures creates uncertain flow between different parts of the company. This poses unknown and unmitigated risks, which could be leveraged as attack vectors and entry points.

### 3.4 Identity and Access management

An important integration issue is the overlapping domains, which results in some users need separate accounts to access multiple services. This leads to multiple services for the same purpose. This also introduces conflicting policies.

- Some users having multiple accounts, both on-prem and cloud.
- Azure AD policy, excludes the use of legacy hardware primarily found in Mediscan
- Inconsistent access rollout to internal file services such as Sharepoint.

Unnecessarily complicated access controls, which would require significant changes to the operation of the company infrastructre.

# 4 Dependency Analysis

## 4.1 Purpose

It is imperative that we're aware who our service providers are, this is to prevent certain types of attacks, such as those aimed at our supply chain. If we don't commit do out due diligence in vetting the providers, we are make ourselves vulnerable, which could undermine the efforts to ensure the safety of the company.

## 4.2 Dependency mapping

From the merger, HLS has inherited a multitude of dependencies. In the section below, the different types are listed:

### 4.2.1 A. Cloud infrastructre Dependencies

- Azure
  - Azure DevOps
  - Azure functions, to deploy custom script for legacy HL7 v2 conversion.
- Google Cloud services

### 4.2.2 B. Identity & Access management Dependencies

- Azure
  - Azure AD
  - Azure AD connect
  - Azure B2C
- On-prem AD

### 4.2.3 C. Application & SaaS Dependencies

- GitHub
- Microsoft Teams
- Slack

### 4.2.4 D. Security & Monitoring Dependencies

- Cisco
  - Cisco ASA firewall, last firmware update from 2020 - legacy
  - multiple managed Cisco ethernet switches
  - VPN - Cisco any connect.
  - VPN - Site-to-Site

### 4.2.5 E. Data processing & Clinical workflow Dependencies

- Azure
  - Azure Blob storage
  - Azure CosmosDB
- Custom solutions
  - C++ device-configuration tool(local)

  - HL7v2 to JSON translation scripts running in Azure functions

- Microsoft
  - OneDrive
  - SharePoint

- DICOM handling

#### 4.2.6 F. Development and Tooling Dependencies

- GitHub
- Terraform

### 4.3 Current providers and dependency severity

| Provider / Service | Jurisdiction | Area | Criticality | Sov. Risk | Lock-in |
|---|---|---|---|---|---|
| Microsoft Azure | US | Cloud compute/storage | High | High | X |
| Azure AD / B2C | US | Identity management | High | High | X |
| Microsoft 365 | US | Collaboration & files | High | High | X |
| GitHub | US | Source code / CI | High | High | X |
| Cisco ASA / VPN | US | Network perimeter | High | Medium | X |
| Cosmos DB | US | Clinical metadata | High | High | X |
| Azure Functions | US | HL7 ingestion | High | High | X |
| Slack | US | Communication (legacy) | Medium | Medium | X |
| Google Cloud | US | Analytics / telemetry | Medium | High | X |
| On-prem AD | EU | Manufacturing IAM | High | Low | X |
| Mediscan tools | EU | Device config | Medium | Low | X |
| AnyConnect VPN | US | Remote access | High | Medium | X |

Table 2: Summary of current providers and sovereignty-related dependency severity.

In table: 2 the columns, *Criticality* refers to the companys current depency on the current implementation. *Sovereignty* Risk explains how much control the company loses over its assets, as they are hosted by these provices, and lastly *Lock-in* asks the question: *"how difficult would it be for the company to replace this service if we needed to?"*.

# 5 Risk Assessment

To anayse how the digital soverignty is impacted LHT's inherited IT-environment, a risk assessment is carried out. It is done by using a impact-likelyhood matrix, seen on figure: 1. This model is comprised of nine sectons, each of a severity level, which ranges from low to critial. This is based on the likehood of occurence and the impact on the company, whether it be operational, legal or stategic.

The axis of the model are impact and likehood, where every step out of the axis increases in the steps, low, medium and high

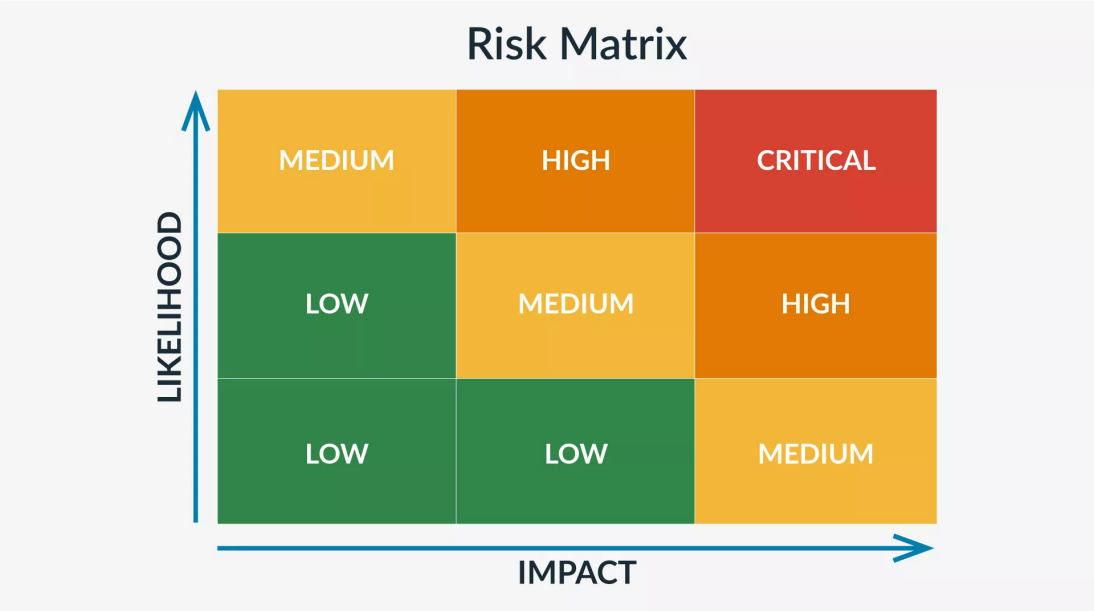


Figure 1: risk vs impact matrix, this is used to visually position LHT's risks. The The product of this matrix is indicated as *severity* in table 3

From this model it is possible to construct a table of the risks, pertaining to the current providers and dependency severity, found in table: 2, following the Methodology: $risk = Likelihood \cdot Impact$. The basis for this Methodology can be found at OWASP[1]. However in this case likelyhood is not only the question, *"will the service break?"*, but also how propable it is, that any impact on this dependency, will bring negative consequences for LHT as a whole?.

Likelyhood can then further be broken down into questions like

- Likelihood of legal or jusrisdictional issues
- Likelihood of operational issues
- Likelihood of vulnerabilities regarding network security
- Likelihood of policy shifting

Given the overall dependency on software and services foreign to the EU, being mainly US based, and given current political climates. It becomes increasingly difficult to narrow down the probablity that foreign governments, might try to leverage services such as these, as political tools.

## 5.1 Physical Vulnerabilities

### 5.1.1 Viby site

The Viby office, inherited from HSM, which implemented rather modern security practices. They rely mainly on Azure as their infrastructre environment, thus, does not indicate any significant physical security risk. However, since physical description of their offices has been supplied, it can only be assumed that they have implemened a minimum of physical office security. This includes thing like:

| Provider / Service | Likelihood | Impact | Severity | Justification |
|---|---|---|---|---|
| Microsoft Azure | MED | HIGH | HIGH | |
| Azure AD / B2C | MED | MED | | |
| Microsoft 365 | LOW | | | |
| GitHub | LOW | | | |
| Cisco ASA / VPN | HIGH | | | |
| Cosmos DB | HIGH | | | |
| Azure Functions | HIGH | | | |
| Slack | LOW | | | |
| Google Cloud | LOW | | | |
| On-prem AD | MED | | | |
| Mediscan tools | HIGH | | | |
| AnyConnect VPN | MED | | | |

Table 3: Summary of current providers and sovereignty-related dependency severity.

- No physical servers
- light network equipment, routers/firewall
- secured doors, with keycards
- auto-lock screensavers
- CCTV of building

It can only be assumed, due to the size and number of employees at HSM pre-merger, that the office was located in a shared-office building. This also points at things they most certainly didn't implement

- Biometric access
- Air-gapped security zones
- Cameras inside the offices
- Monitoring desk environments
- audit trails

These are things that more likely relate to ISO 27001[2], style physical access control, which, due to their environments and workflows, most likely didn't require.

#### 5.1.2 Lystrup site

The Lystrup manufacturing site, inherited from Mediscan, with dedicated engineering and manufacturing environment, though it has been updated and improved over time. It still exposes several weakness, which has arisen from aging equipment.

- Basic server room with no biometric access, meaning anyone with a keycard can enter the room
- Basic UPS with a ambient cooling and a mix of new and old equipment. No temperature of server equipment impacts lifespan and reliability
- Cisco ASA firewall, unpatched since 2020. This particular model of switch is vulnerable to a remote attack, which enables an attacker to gain memory content[3]
- legacy on-prem AD with no MFA, can be exploited to gain unrestricted access
- Physical access also allow the physical removal of decades of documentation, which could lead to IP theft.

### 5.2 How Identified Risks Impacts LHT's Digital Soverignty

The risks highlighted shows that the current landscape of LHT's sovereignty, is primarily dictated by foreign, non-EU cload platforms, which includes a wide span of roles and services. From the development environments, to azure AD and data processing, because these are US based companies, they have to comply with legislation, such as the CLOUD act[4] and FISA_702[5]

# 6 EU-Alternatives

# 7 Comparison of current and proposed solution

# 8 recommended migration strategy

# 9 conclusion

# References


[1] OWASP. *OWASP Risk Rating Methodology*. 2025. URL: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology (visited on 12/10/2025).

[2] www.iso.org. *ISO/IEC 27001:2022*. 2025. URL: https://www.iso.org/standard/27001 (visited on 12/11/2025).

[3] sec.cloudapps.cisco.com. *Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web Services Information Disclosure Vulnerability*. 2025. URL: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-info-disclose-9eJtycMB (visited on 12/11/2025).

[4] Government of the United States. *CLOUD Act*. 2025. URL: https://www.justice.gov/criminal/cloud-act-resources (visited on 12/11/2025).

[5] Government of the United States. *Foreign Intelligence Surveillance Act, FISA section 702*. 2025. URL: https://www.intel.gov/foreign-intelligence-surveillance-act/fisa-section-702 (visited on 12/11/2025).