Security architecture specification

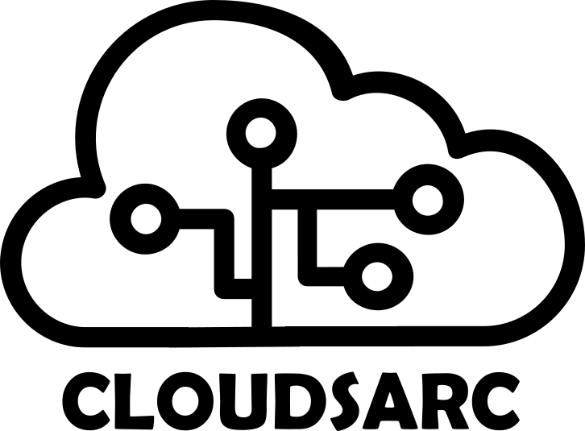
[](https://www.cloudsarc.org/)

Table of contents

[Executive Summary 4](#_Toc83720730)

[Terms and abbreviations 4](#_Toc83720731)

[1 Introduction 5](#_Toc83720732)

[1.1 Background 5](#_Toc83720733)

[1.2 Scope 5](#_Toc83720734)

[2 Methodology 5](#_Toc83720735)

[3 Business- and regulatory requirements 6](#_Toc83720736)

[3.1 Business requirements 7](#_Toc83720737)

[3.2 Regulatory requirements 7](#_Toc83720738)

[4 Strategy and goals 8](#_Toc83720739)

[4.1 Goals 9](#_Toc83720740)

[4.1.1 Target cloud security architecture 9](#_Toc83720741)

[4.1.2 Cloud foundation 9](#_Toc83720742)

[4.1.3 Security initiatives 9](#_Toc83720743)

[4.1.4 EMR system 10](#_Toc83720744)

[4.1.5 Development environments 10](#_Toc83720745)

[4.1.6 Clinical solutions 10](#_Toc83720746)

[5 Security requirements 10](#_Toc83720747)

[6 Risk and mitigation 12](#_Toc83720748)

[6.1 Risk scenarios 12](#_Toc83720749)

[6.2 Risk matrix 13](#_Toc83720750)

[6.3 Risk mitigation 14](#_Toc83720751)

[7 Compliance 16](#_Toc83720752)

[7.1 GDPR 16](#_Toc83720753)

[7.2 HIPAA 17](#_Toc83720754)

[8 Security measures and resilience 17](#_Toc83720755)

[8.1 Defense in depth layers 17](#_Toc83720756)

[8.1.1 GRC Management 17](#_Toc83720757)

[8.1.2 Identity and access 17](#_Toc83720758)

[8.1.3 Security ops& Infrastructure 18](#_Toc83720759)

[8.1.4 Endpoint 18](#_Toc83720760)

[8.1.5 Application 18](#_Toc83720761)

[8.1.6 Data 18](#_Toc83720762)

[8.2 Defense in depth circle 18](#_Toc83720763)

[References 20](#_Toc83720764)

| Version | Date | Change comments | Author | Approved |
| --- | --- | --- | --- | --- |
| 0.1 | 01.01.2021 | First edition | Lead architect | CEO |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Executive Summary

*[Create a summary of all the important aspects throughout the remainder of the cloud security strategy document. Share this section with the executive team to communicate the essence of your cloud security strategy. The text below is just an example, and it must be customized based on your specific context.]*

This document defines the health sector cloud security strategy. In the health sectors business plan for 2019 – 2023, important objectives are communication across health entities, exchange of health information and patient communications. These objectives can be met utilizing cloud based services compliant with the health sector regulations.

The health sector must become a modern provider of IT services to the clinical institutions throughout the nation and must therefore adapt to the market and the need to be able to deliver services faster and in new ways. At the same time, the threat landscape is changing and more resources and competencies are needed to stay secure and compliant in the cloud.

To deliver cloud services to clinics in the health sector a solid security architecture is necessary to protect sensitive data across all services. A hybrid cloud deployment model is preferred along with a focus on SaaS and PaaS service models. Operations in the cloud will need a CCOE who can centralize and automate tasks and stay updated on the latest technology trends.

The health sectors strategy for using cloud services follows these principles:

* Cost efficiency
* Flexibility and capacity
* Quality
* Security

## Terms and abbreviations

|  |  |
| --- | --- |
| **Term** | **Description** |
| SaaS | Software As A Service |
| PaaS | Platform As A Service |
| IaaS | Infrastructure As A Service |
| CSA CCM | Cloud Security Alliance Cloud Controls Matrix |
| GDPR | General Data Protection Regulation |
| PHI | Protected Health Information |
| NIST CSF | National Institute of Standards and Technology Cybersecurity Framework |
| IaC | Infrastructure as Code |
| DevOps | DevOps is a set of practices that combines software development (Dev) and IT operations (Ops). |
| CCOE | Cloud Center Of Excellence |
| SOC | Security Operations Center |

# Introduction

*[Explain the background for the architecture initiative define the scope. The text below is just an example, and it must be customized based on your specific context.]*

This document describes the cloud security architecture for the Cloudsarc Health Clinic. The security architecture is created from the business- and regulatory requirements for the health clinics cloud environment. The outcome of the architecture work is a set of security measures selected for risk mitigation, cloud environment resilience and for covering the business requirements.

## Background

The Cloudsarc Health Clinic needs an online EMR system operating in a cloud environment. The system will serve both clinicians, administrators and patients and will contain personal information and health information.

## Scope

The security architecture described in this document will cover the security requirements and measures for the health clinic cloud environment. EMR requirements for authentication and access control will be covered, but not the EMR system requirements in general. The security architecture contains security measures at the NIST CSF [1] sub-category level that can be mapped to cloud provider specific services, but these services are not covered in this document.

# Methodology

*[The Cloudsarc methodology is used for creating the security architecture described in this document. You can customize the methodology to suit your own needs. The text below is just an example, and it must be customized based on your specific context. ]*

Business requirements and regulatory requirements are important for cloud security architecture. These requirements set the context for the requirement work and are mapped to security requirements.

A risk assessment is performed using an assessment methodology based on NIST 800-30 guidance document. Se chapter 6 for a description of the risk analysis.

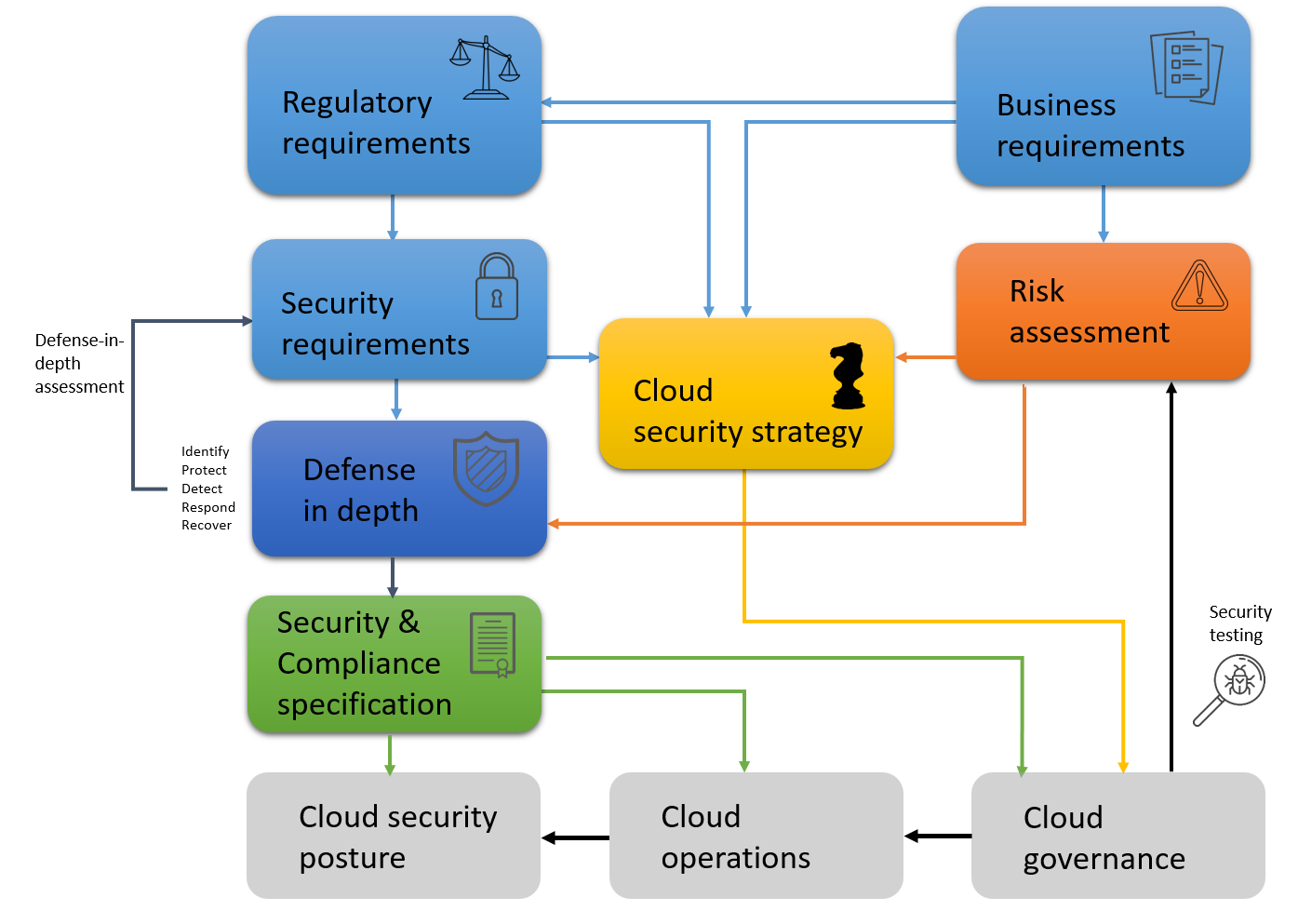
A cloud strategy is created using output from the risk assessment process and security requirement process. Se chapter 4 for a description of strategy and goals.

A defense-in-depth analysis is performed using NIST CSF functions and architectural layers as a foundation. If gaps are uncovered, they will be inserted into the requirements list and mapped to securtity measuers to complete the cloud security posture. See chapter 7 for a description of security measures and resilience.

A compliance mapping done, in this example to GDPR and HIPAA. Use the NIST CSF mappings workbook to find the right mappings for the security measures.

From this document, we can implement the architecture in a cloud platform from for example Azure, Google Cloud or Amazon web services.

Security testing should be performed on at least annual basis and will give valuable input to subsequent risk analysis of the environment.

**

# Business- and regulatory requirements

*[The business and regulatory requirements in this chapter is based on the Cloudsarc health clinic example. Customize the requirements lists for use in your own projects.The text below is just an example, and it must be customized based on your specific context. ]*

The cloudsarc health clinic runs their Electronic Medical Records, EMR, in a public cloud.

As the records naturally contain PHI there will be many business and regulatory requirements that dictates a strong security posture in the clinics cloud environment.

## Business requirements

The business requirements reflects the users business needs when they perform their work functions. The cloud environment must deliver functionality to the users that meet the listed business requirements.

|  |  |
| --- | --- |
| **Req#** | **Requirement description** |
| R1 | The clinical portal must provide efficient communication between all actors |
| R2 | The solution must offer appointment booking and be available to patients, administrators and clinicians |
| R3 | The solution must be able to handle storage and retrieval of sensitive health data for patients |
| R4 | Applications must be highly available, also on mobile devices |
| R5 | Cost effective operations and application delivery mechanisms |
| R6 | The solution must be able to scale quickly to handle more users |
| R7 | The solution must be able to track patient demographics |
| R8 | Functionality for medical billing must be provided |
| R9 | Functionality for creating reports medical and financial data must be available |
| R10 | The solution must offer rich editing capabilities for journal documents |
| R11 | The solution must provide functionality for prescribing drugs |
| R12 | The solution should offer functionality for forms and clinical notes |
|  |  |
|  |  |

## Regulatory requirements

Naturally, a health clinic will also need to have security and compliance requirements

A health clinic process information on behalf of patients. The patient data is personal information and health information. Health information is considered sensitive personal information and must be protected.

HIPAA [2] compliance is mandatory for health clinics in the US, GDPR [3] mandatory in Europe.

In addition to regulatory requirements, the health clinic operation in the cloud must be protected from attack from adversaries. This means that security and privacy requirements stated by HIPAA and GDPR will not be sufficient to protect the cloud based electronic medical record (EMR) system. See chapter 7 for resilience against adversaries.

|  |  |  |
| --- | --- | --- |
| **Req#** | **Regulation** | **Requirement description** |
| LR1 | GDPR | Document who has access to PHI and the processing activities |
| LR2 | HIPAA | All changes to PHI must be traceable |
| LR3 | GDPR | Document the legal justification for processing PHI |
| LR4 | GDPR | PI and PHI should be encrypted when possible |
| LR5 | GDPR | Conduct a data protection impact assessment (DPIA) |
| LR6 | HIPAA | An access control mechanism must be used to protect PHI |
| LR7 | HIPAA | Data must be encrypted at rest and in transit |
| LR8 | HIPAA | Policies must be devised and implemented to restrict the use of workstations that have access to PHI |
| LR9 | HIPAA | Create a business continuity plan (BCDR) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Strategy and goals

*[Strategy and goals are based on the Cloud Secuirty Strategy document. Create your own strategy and update this chapter to reflect your own priorities. The text below is just an example, and it must be customized based on your specific context. ]*

The health clinic must become a modern provider of IT services to meet new requirements for communication and innovative service delivery and must therefore adapt to the market and the need to be able to deliver services faster and in new ways. At the same time, the threat landscape is changing and more resources and competencies are needed to stay secure and compliant in the cloud.

To deliver cloud services to the health clinic, a solid security architecture is necessary to protect sensitive data across all services. A public cloud deployment model is preferred along with a focus on SaaS and PaaS service delivery models. Operations in the cloud will need a Cloud Center Of Excellence (CCOE) who can centralize and automate tasks and stay updated on the latest technology trends.

The health clinics strategy for using cloud services follows these principles:

* Cost efficiency
* Flexibility and capacity
* Quality
* Security

## Goals

### Target cloud security architecture

A holistic architecture must be created including principles, criteria and requirements for the choice and use of cloud solutions for the health clinic. Principles applies to how services are organized, designed, secured and delivered. It must be stated how different delivery models should be organized and integrated into the total service offering, information management and application architecture.

### Cloud foundation

A Cloud Foundation framework must be established before services are offered to end-users. The Cloud Foundation framework requires the following:

* Identity management and governance model established for cloud services
* Security requirements for cloud services specified
* Economy model established
* New management model prepared
* Organizational changes implemented

### Security initiatives

The following security initiatives must be completed before cloud services are deployed:

* The chosen cloud provider’s security practices following the shared responsibilities model (as described in Appendix A) and the CSA CCM are verified
* Infrastructure and application security are modernized and cloud native by using IaC and DevOps
* A modern perimeter using centrally managed identity controls to protect data, devices and accounts is established
* A SOC covering detection and response for cloud security incidents is created
* Other security measures from the risk analysis in chapter 4:
  + Investigate cloud provider IaaS and PaaS services for portability
  + Enforce policies for multifactor authentication
  + Enforce least privilege for authorization of personnel
  + Encrypt all traffic to the cloud environment
  + Develop internal cloud security competencies

### EMR system

The EMR system for the health clinic can be provided when the following sub-goals are met:

* Governance model for the cloud environment specified
* Governance is established for the EMR system
* All risk mitigation measures are implemented and verified
* The EMR system is tested and approved

### Development environments

Developers need a modern development process to utilize the cloud for development of new healthcare solutions. The following must be completed:

* Architecture, security and management model prepared for PaaS / IaaS
* A solid DevOps process with focus on security

### Clinical solutions

Clinical solutions offered to patients is an important goal in the strategy but requires data protection and compliance. Architectural work needs to be completed before services are developed and deployed.

* Architecture, security and management model are prepared for clinical solutions
* Platform for virtual health services established as a cloud service

# Security requirements

*[The security requirements in this chapter are based on the security requirements for the Cloudsarc health clinic Create your own security requirements and list them in the table below along with relevant mappings.The text below is just an example, and it must be customized based on your specific context. ]*

Security requirements for the Cloudsarc health clinic represents the high level security requirement. These will be derived from Business- and regulatory requirements as described in chapter 3.

We will use the NIST NSF categories and sub-categories as guidelines for selecting appropriate security requirements for the clinic.

All selected security requirements must be relevant for the health clinic it will be our job to illustrate this relevance to management to get funding for the security initiative.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sec req #** | **Description** | **Req.#** | **Legal Req.#** | **NIST CSF Categories** |
| S1 | Sufficient confidence in the actors' identity and strong authentication | R1, R2, R3 |  | PR.AC |
| S2 | Access to information based on ownership or service needs | R1, R2, R3, R10, R11, R12 | LR1, LR2, LR6 | PR.AC |
| S3 | Traceability for all operations on PHI in the clinical platform | R3, R10, R11, R12 | LR1, LR2 | DE.CM |
| S4 | Granular role-based access control | R1, R2, R3, R8, R9, R10, R11, R12 | LR6 | PR.AC |
| S5 | Protection of sensitive data from unauthorized disclosure using encryption | R3, R4, R5 | LR4, LR7 | PR.DS |
| S6 | High availability - according to the criticality of the solution | R6 |  | PR.DS, PR.IP |
| S7 | Change management adapted to cloud delivery | R5 |  | PR.IP |
| S8 | Business continuity and disaster recovery must be addressed in the solution infrastructure | R5,R6 | LR9 | ID.SC, PR.IP, RC.RP,RC.IM, RC.CO |
| S9 | Utilize cloud services for cost effective and secure operations | R5 |  | PR.IP |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Risk and mitigation

*[The risks and mitigations in this chapter is based on the Cloudsarc health clinic example. Perform your own risk assessment and find mitigation measures. The text below is just an example, and it must be customized based on your specific context. ]*

For the Cloudsarc health clinic there are many types of risk. The clinic is available over the internet and processes sensitive data. This means that it could be a target for advanced hackers. There will always be risks when processing sensitive data, and it is our job as cloud security architects to identify, analyze and prioritize these risks.

## Risk scenarios

These risk scenarios are risk scenarios for the Cloudsarc health clinic.

In most of these scenarios, that all have a high risk severity, the threat actors are sophisticated attackers. Sophisticated attackers is in this context either organized criminals or state sponsored hackers.

The target of these potential attacks are PHI and the impact is rated as severe in most of the scenarios.

The column for NIST CSF function to illustrate where the focus must be put for risk mitigation.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Risk #** | **Risk scenario** | **NIST CSF Function** | **Likelihood** | **Impact** | **Risk Severity** |
| Ri1 | Sophisticated attackers or malicious insiders can steal, modify or delete PHI due to misconfiguration of cloud security settings | Protect | 4 | 4 | Very High |
| Ri2 | Sophisticated attackers can render data unavailable and by installing ransomware. PHI can be lost because a recovery plan has not been created. | Recover | 3 | 4 | Very High |
| Ri3 | Sophisticated attackers and exploit insecure APIs and steal, modify or delete PHI. | Protect | 3 | 4 | Very High |
| Ri4 | Sophisticated attackers could hijack a user account and steal, modify or delete PHI | Protect | 3 | 4 | Very High |
| Ri5 | Due to lack of segregation of responsibilities a malicious insider can read PHI for some patients | Protect | 2 | 2 | Moderate |
| Ri6 | Sophisticated attackers can steal, modify or delete PHI due to inadequate security monitoring for detecting suspicious and unauthorized activities. | Detect | 2 | 4 | High |
| Ri7 | Sophisticated attackers can steal, modify or delete PHI by continuing attacks and hiding evidence because logs are not collected and aggregated in a central location | Detect | 2 | 4 | High |
| Ri8 | Sophisticated attackers can render data unavailable and by installing ransomware. PHI can be lost because an incident response plan has not been tested. | Response | 2 | 4 | High |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## Risk matrix

When we illustrate the risks in the risk matrix, it is very easy to get a good understanding of the current situation concerning risk.

We can clearly see what risk elements that needs to be mitigated before the EMR system is approved for use.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Impact | **Very High 4** |  | Ri6, Ri7, Ri8 | Ri2,Ri3, Ri4 | Ri1 |
| **High 3** |  |  |  |  |
| **Moderate 2** |  | Ri5 |  |  |
| **Low 1** |  |  |  |  |
|  | | **Low 1** | **Moderate 2** | **High 3** | **Very High 4** |
| Likelihood | | | |

## Risk mitigation

Risk 1 contains the following scenario:

Sophisticated attackers or malicious insiders can steal, modify or delete PHI due to misconfiguration of cloud security settings.

As cloud misconfiguration is a common risk for cloud deployments there are many good sources to information about risk mitigation. The Cloud Security Alliance (CSA) Top Threats to Cloud computing, cloud controls matrix and NIST CSF are used to identify good security measures for mitigating this risk.

As you can see there are 16 mitigations spread across four functions of the NIST CSF.

Risk 2 in our assessment has the following scenario:  
Sophisticated attackers can render data unavailable and by installing ransomware. PHI can be lost because a recovery plan has not been created.

In this scenario we focus on the problem of improper recovery. As ransomware encrypt our files and causes complete unavailability, a good recovery plan is vital to bring our health clinic online,

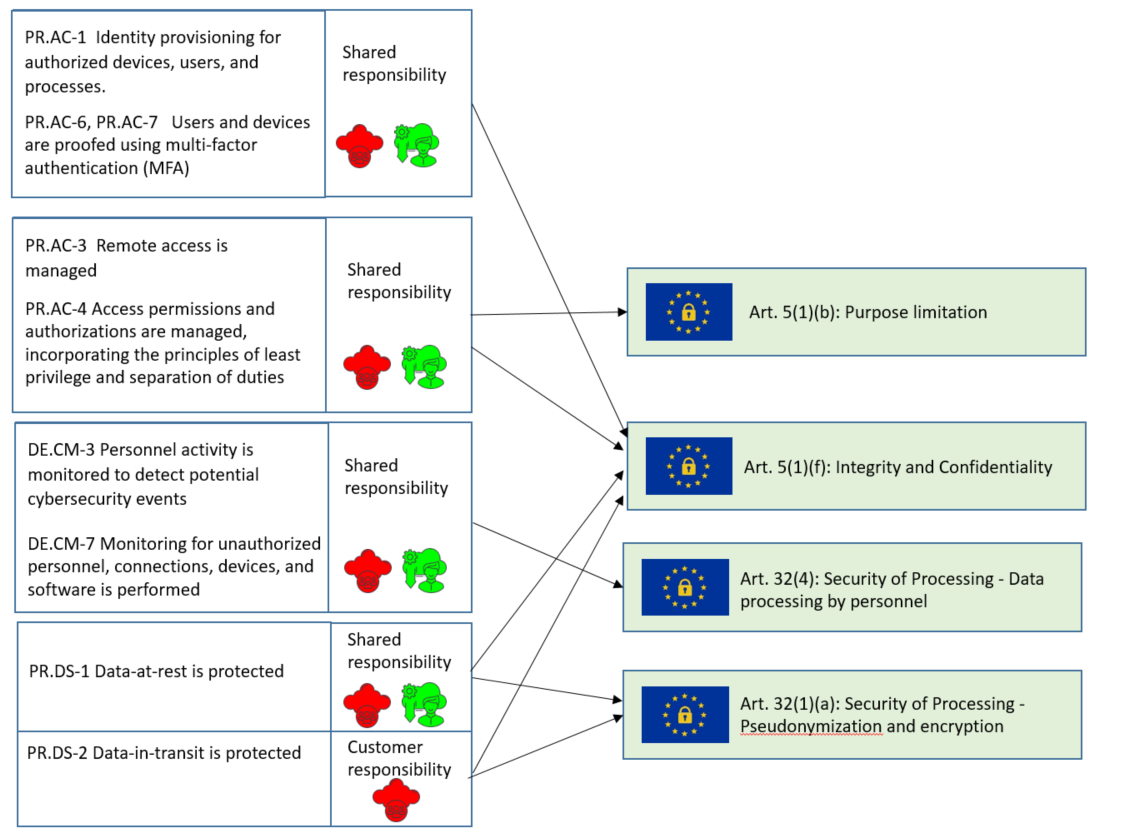
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk #** | **Risk scenario** | **Risk rating** | **Mitigation ID#** | **Risk mitigation measures (NIST CSF Sub-Categories)** |
| Ri1 | Sophisticated attackers or malicious insiders can steal, modify or delete PHI due to misconfiguration of cloud security settings. | Very High | Mi1 | ID.AM-3,ID.AM-4, ID.AM-5 |
| Mi2 | ID.BE-1, ID.BE-5  ID.GV-4 |
| Mi3 |
| Mi4 | ID.RA-1,ID.RA-3,ID.RA-4, ID-RA-5, ID.RA-6 |
| Mi5 | ID.RM-1,ID.RM-2, ID.RM-3 |
| Mi6 | PR.AC-1,PR.AC-4, PR.AC-5 |
| Mi7 |
| PR.AT-1,PR.AT-2,PR.AT-4,PR.AT-5 |
| Mi8 | PR.DS-1,PR.DS-2, PR.DS-3, PR.DS-5, PR.DS-6,PR.DS-7 |
| Mi9 |
| PR.IP-1,PR.IP-2,PR.IP-3, PR.IP-7,PR.IP-8 PR.IP-12 |
| Mi10 |
| PR.PT-2,PR.PT-4 |
| Mi11 |
| DE.AE-1,DE.AE-2,DE.AE-3,DE.AE-4 |
| Mi12 |
| DE.CM-1, DE.CM-3, DE.CM-4,DE.CM-5, DE.CM-6, DE.CM-7 |
| Mi13 |
| DE.DP-2,DE.DP-3,DE.DP-4,DE.DP-5 |
| Mi14 |
| RS.CO-2,RS.CO-3 |
| Mi15 |
| RS.AN-1 |
| Mi16 | RS.MI-3 |
| Ri2 | Sophisticated attackers can render data unavailable and by installing ransomware. PHI can be lost because a recovery plan has not been created. | Very High | Mi17 | RC.RP-1 |
| Mi18 | RC.CO-1, RC.CO-2, RC.CO-3 |
|  |  |  |  |  |

# Compliance

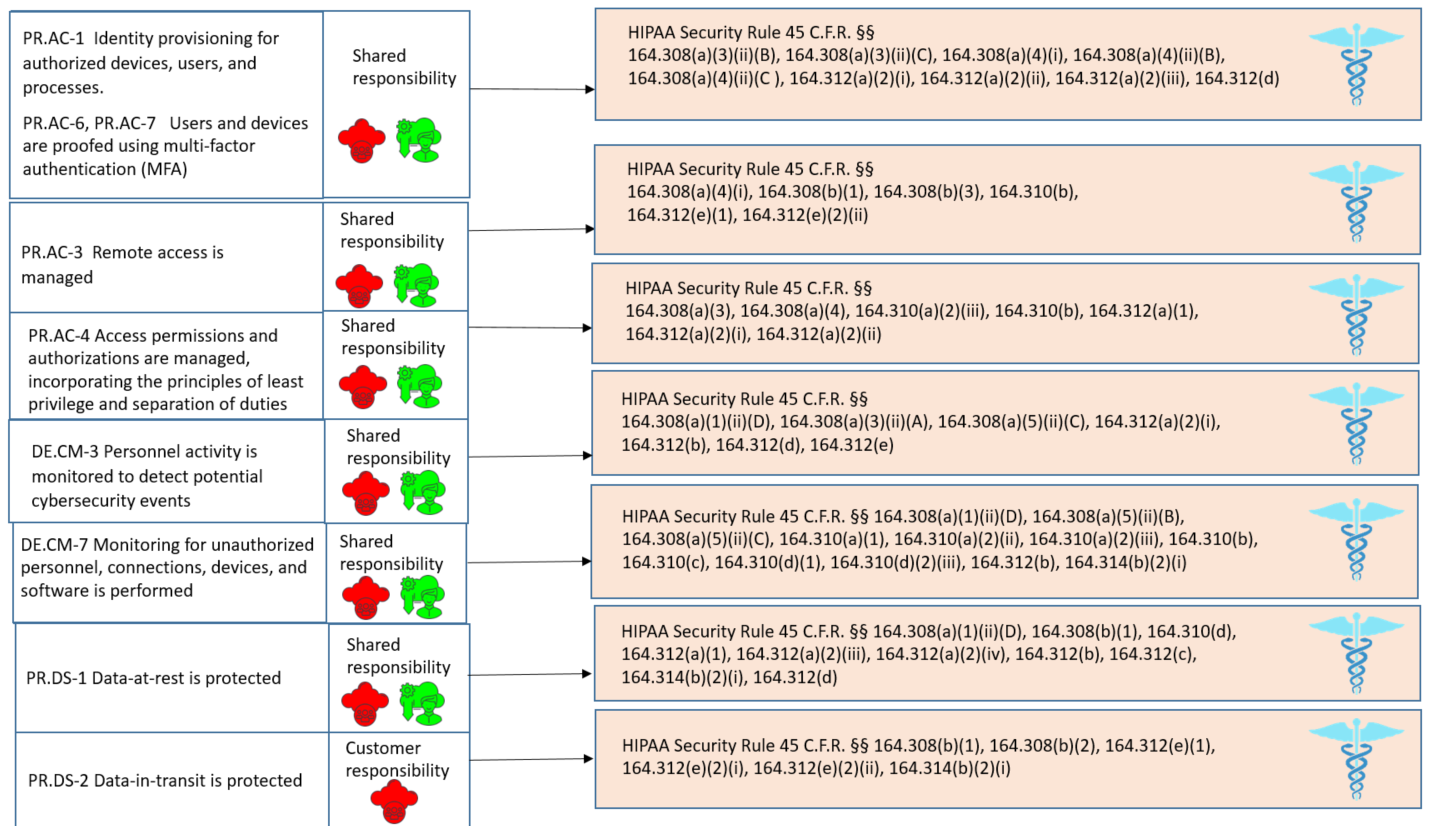
*[Create your own graphical mappings of security measures to regulations or just use the attached spreadsheet to create mappings for your own project. The text below is just an example, and it must be customized based on your specific context. ]*

This chapter describe mappings to GDPR and HIPAA. Compliance with regulations is important for the Cloudsarc health clinic and this specification along with attached mapping spreadsheets will provide information on how the security requirements support GDPR and HIPAA

## GDPR



## HIPAA



# Security measures and resilience

*[The defense in depth approach in this chapter is based on the Cloudsarc health clinic example. Customize the defense in depth strategy for use in your own projects and use the suggested visualization for stakeholder communication. The text below is just an example, and it must be customized based on your specific context. ]*

## Defense in depth layers

### GRC Management

Governance, Risk and Compliance is the overall management of the cloud security program ensuring we have the right security measures to lower the total risk.

The CCOE has the responsibility for governance, risk and compliance and will also manage the development of security architecture for the cloud. The CCOE will manage cloud security personnel and capabilities for detection, response and recovery.

### Identity and access

Identity and access management is important as a layer of defense in the cloud. We are moving from a world with perimeter defenses to a world where identity is the new perimeter. Strong identity and access management processes are vital for success in the cloud.

Cloud provider tools for identity and access management should be used to handle identities and access to assets effectively throughout the cloud environment.

### Security ops& Infrastructure

Day-to-day operations of security countermeasures to protect assets is important also in the cloud. The infrastructure must be monitored for intrusion attempts 24/7 and tools for automation.

SecaaS tools from your chosen cloud provider should be utilized to run your security operations in the cloud.

### Endpoint

Endpoints are even more important when moving to the cloud. Protection of mobiles, laptops and tablets is important for protection of the assets in the cloud. The endpoints should be scanned for vulnerabilities, automatically patched and anti-virus software must be installed.

An emerging trend is to upload endpoint security logs to the cloud for aggregation and analysis.

### Application

A secure development process is key also in the cloud. Security must be built into applications from the beginning along with privacy. Attacks against applications running in the cloud exploit vulnerabilities in applications to gain access to your assets.

Protections against attacks on the application layer can be mitigated using a Web Application Firewall.

### Data

It is important to protect data both at rest and in transit. Encryption of traffic and data in cloud storage are good mitigations to protect data from many different types of attacks.

The cloud provider offers many mechanisms for encryption and key management.

## Defense in depth circle

*[You can use defense in depth circle below in your own projects. The security requirements and mitigations are placed as objects and you can change these to document your own security posture. The text below is just an example, and it must be customized based on your specific context. ]*

We have five sectors of the circle, each representing a NIST CSF function. We also have six circles representing each architectural layer.

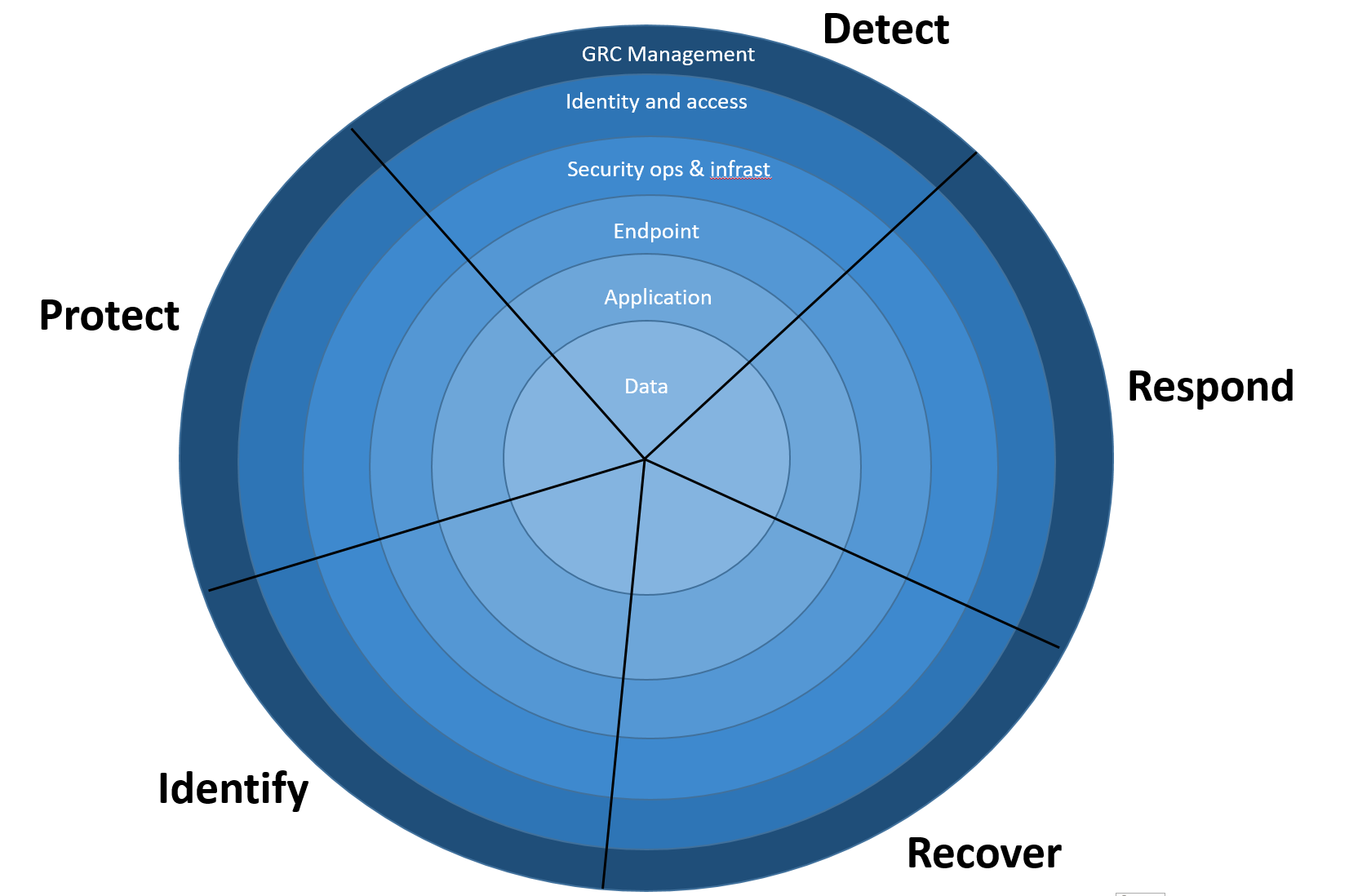
The idea is to visualize the defense in depth coverage using this circle. The more circles that are filled with security measures of each sector, the better. However, the circle does not need to be completely full to represent a good security posture.

The mitigations marked in green are placed in the defense in depth circle. These represent the risk mitigations and are meant to bring down an unacceptable risk to an acceptable level. At the same time, these mitigations help us improve the resiliency of the security architecture. Most of the circles in each sector are actually containing at least one mitigation. When all mitigations from the risk assessment is in place, you will see that there is a significant overlap between different mitigations.

The most important reason to go through all mappings and risk assessment is not only to invest resources in what we need the most, but also to document why we have to do it.

A lot of the information from risk scenarios, security and regulatory requirements will also be valuable when we start selecting various security services from our chosen cloud provider.

During an audit you will be asked to show your risk assessments, security requirements and compliance status. I will talk more about compliance in the next section.



Mi18

Mi17

S8

Mi17

Mi17

Mi14

Mi16

Mi15

Mi15

Mi15

Mi15

Mi1

Mi1

Mi1

Mi1

S8

Mi2

Mi3

Mi4

Mi5

Mi6

S8

S5

S6

Mi8

Mi10

Mi10

Mi9

Mi7

S4

S2

S1

S7

Mi11

Mi12

Mi12

Mi12

S3

Mi13

Mi11

Mi11

# References

|  |  |
| --- | --- |
| [1] | N. I. o. S. a. Technology, "NIST CYBERSECURITY FRAMEWORK," [Online]. Available: https://www.nist.gov/cyberframework. |
| [2] | U. D. o. H. &. H. Services, "Health Insurance Accountability and Portability Act," [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/index.html. |
| [3] | E. Union, "General Data Protection Regulation," [Online]. Available: https://gdpr-info.eu/. |