

TALLINN UNIVERSITY OF TECHNOLOGY

School of Information Technologies

IT College

Benedek Matveev 201840IVSB

**The NIST SP 800-53 Revision 5 Standard  
Compliance at an IT Startup: an Applicability  
Analysis and Implementation**

Bachelor Thesis

**Supervisor**

Kaido Kikkas

PhD

**Co-supervisor**

Gabor Jeney

PhD

TALLINNA TEHNIKAÜLIKOOL

Infotehnoloogia teaduskond

IT Kolledž

Benedek Matveev 201840IVSB

**NIST SP 800-53 standardi versiooni 5  
rakendamine IT-idufirmas: sobivusanalüüs ja  
realisatsioon**

Bakalaureusetöö

**Juhendaja**

Kaido Kikkas

PhD

**Kaasjuhendaja**

Gabor Jeney

PhD

## **Author's declaration of originality**

I hereby certify that I am the sole Author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author:       Benedek Matveev

.....

(Signature)

Date:         05.01.2023

# **Abstract**

In the case of startups who utilise cloud-based infrastructure, there is no up-to-date open-source implementation and applicability analysis of technologies, tools, methodologies, and guidelines that will assist them in complying with the NIST SP 800-53 Rev. 5 standard. The purpose of this thesis is to model a simplified IT infrastructure and mobile application that handles user data, as well as to find solutions to comply with the relevant controls of NIST SP 800-53 Rev. 5 standard.

# **Annotatsioon**

Pilvepõhist infrastruktuuri kasutavate idufirmade puhul puudub tehnoloogiate, tööriistade, meetodikate ja juhiste ajakohane avatud lähtekoodiga juurutamise ja rakendatavuse analüüs, mis aitaks neil järgida NIST SP 800-53 Rev. 5 standard. Käesoleva lõputöö eesmärk on modelleerida lihtsustatud IT-infrastruktuuri ja mobiilirakendust, mis käitleb kasutajaandmeid, samuti leida lahendusi NIST SP 800-53 Rev. 5 standardi vastavate juhtelementide täitmiseks.

## List of abbreviations and terms

ABAC	Attribute-Based Access Control
API	Application Programming Interface
AWS	Amazon Web Services
BGP	Border Gateway Protocol
BIOS	Basic Input/Output System
CA	Certificate Authority/Certificate Authorities
CaaS	Container as a service
CAC	Common Access Card
CAVP	Cryptographic Algorithm Validation Program
CIRT	Computer Incident Response Team
CISA	Cybersecurity and Infrastructure Security Agency
CMVP	Cryptographic Module Validation Program
CONOPS	Concept of Operations
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoS	Denial of Service
EAP	Extensible Authentication Protocol
FTP	File Transfer Protocol

GPS	Global Positioning System
HTTP	Hypertext Transfer Protocol
I/O	Input/Output
IaaS	Infrastructure as a Service
ICS	Industrial Control System
IEEE	Institute of Electrical and Electronics Engineers
IOC	Indicators of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
ITL	Information Technology Laboratory
MAC	Media Access Control
MLS	Multilevel Secure
MTTF	Mean Time To Failure
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards in Technology
OPSEC	Operation Security
OS	Operating System
OVAL	Open Vulnerability and Assessment Language
PaaS	Platform as a Service
PDF	Portable Document Format
PDS	Position Designation System
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RBAC	Role-Based Access Control
RD	Restricted Data
RFID	Radio-Frequency Identification
RFP	Request For Proposal
RPKI	Resource Public Key Infrastructure

SaaS	Software as a Service
SAP	Special Access Program
SCAP	Security Content Automation Protocol
SCRM	Supply Chain Risk Management
SDLC	System Development Life Cycle
SIEM	Security Information and Event Management
SMTP	Simple Mail Transfer Protocol
SOC	Security Operations Center
SP	Special Publication
SWID	Software Identification
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
UEFI	Unified Extensible Firmware Interface
UPS	Uninterruptible Power Supply
UTC	Coordinated Universal Time
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
XML	Extensible Markup Language



# Table of Contents

<b>1. Introduction .....</b>	<b>1</b>
1.1. Problem statement.....	1
1.2. Scope and limitations .....	2
1.3. Methodology.....	3
<b>2. Background.....</b>	<b>4</b>
2.1. Overview of the NIST SP 800-53 Rev. 5 standard.....	4
2.1.1. Supporting documents.....	5
2.1.2. Families and control structure .....	6
2.1.3. Reasons for choosing the standard.....	7
2.2. Overview of the startup model .....	8
2.2.1. Selection of the IaaS platform .....	8
2.2.2. Components of the infrastructure.....	9
2.2.3. Overview of the Azure IaaS platform .....	11
<b>3. Control selection .....</b>	<b>13</b>
3.1. Selection methodology of applicable controls.....	13
3.2. Merging Azure policies with the selected controls.....	14
<b>4. Applicability Analysis and Implementation .....</b>	<b>16</b>
4.1. Azure infrastructure compliance.....	17
4.1.1. Azure Policy Service.....	18
4.1.2. Microsoft Defender for Cloud .....	21
4.1.3. Microsoft Sentinel Service .....	24
4.2. Non-IaaS component compliance .....	26
4.2.1. Domain Name Hosting.....	26
4.2.2. DNS Settings: .....	27
4.2.3. SSL/TLS .....	27
4.2.4. Security Setings .....	28
<b>5. Results .....</b>	<b>30</b>
5.1. Azure infrastructure compliance results.....	30
5.1.1. Azure Policy Service.....	30
5.1.2. Microsoft Defender for Cloud .....	31
5.1.3. Microsoft Sentinel Service .....	32
5.2. Cloudflare Compliance Results .....	33

5.2.1. DNS Settings: .....	33
5.2.2. SSL/TLS .....	34
5.2.3. Security Setings .....	35
<b>6. Summary.....</b>	<b>38</b>
6.1. Conclusion.....	38
6.2. Further works.....	39
<b>Acknowledgements.....</b>	<b>40</b>
<b>Bibliography .....</b>	<b>41</b>
<b>Appendices.....</b>	<b>44</b>
Appendix 1 – Non-Exclusive License .....	44
Appendix 2 – Supporting Tables:.....	45
1. NIST SP 800-53 Revision 5 Control Families Table:.....	45
2. Table of Selected Controls: .....	46

# List of Figures

Figure 1. Control structure [8] .....	7
Figure 2. Detailed support of controls [12] .....	9
Figure 3. Microsoft Azure Platform TestVM_group .....	12
Figure 4. Control Catalog (spreadsheet) (xls) for the SP 800-53 Rev. 5 standard.....	13
Figure 5. Control Baselines spreadsheet (xls) for SP 800-53B Rev. 5.....	13
Figure 6. Selected Controls.....	14
Figure 7. Selected controls with azure policies .....	15
Figure 8. Policy   Definitions.....	19
Figure 9. Initiative of selected controls .....	20
Figure 10. Microsoft Defender for Cloud Regulatory compliance .....	22
Figure 11. Applied initiatives .....	23
Figure 12. Configuration change deployment .....	23
Figure 13. Microsoft Sentinel   Content hub.....	25
Figure 14. Control overview in Microsoft Sentinel .....	25
Figure 15. Cloudflare DNS settings.....	27
Figure 16. Cloudflare SSL/TLS settings .....	28
Figure 17. Security posture after configuration changes .....	30
Figure 18. Policy compliance after configuration changes.....	31
Figure 19. Microsoft Defener for Cloud after configuration changes.....	31
Figure 20. Microsoft Sentinel SC-5 control after configuration changes .....	32
Figure 21. Microsoft Sentinel SC-7 control after configuration changes .....	32
Figure 22. Cloudflare DNS with changed settings.....	34
Figure 23. Cloudflare SSL/TLS with changed settings .....	35
Figure 24. Cloudflare Security - WAF changed settings .....	36
Figure 25.. Cloudflare Security - DDoS changed settings .....	37

# List of Tables

Table 1. SC-7 noncompliant policies .....	21
Table 2. List of control families [25] .....	46
Table 3. List of selected controls .....	48

# 1. Introduction

## 1.1. Problem statement

Cloud computing [1] solutions occupy an increasing market share, providing technologies like IaaS, PaaS, SaaS, and CaaS. Statistics predict that cloud adoption among enterprise organisations will overtake on-premises solutions [2] [3]. During building their infrastructure, startups and newly established companies will be more likely to utilise cloud computing due to natural scaling.

To protect shareholders and customers, these companies will be required to comply with one or more cyber security standards as their user base grows, handles more data or becomes more popular. The NIST SP 800-53 is one of the world's most widely accepted and used open-source cyber security standards.

The problem is that cyber security standards consist of a list of controls without detailed guidance on implementing each control. Although many companies offer compliance preparation services, no open-source analysis is available to assist startups in complying with NIST SP 800-53 Revision 5 standard.

This thesis is intended to model a cloud-based infrastructure similar to what startups use, and provide an analysis of the applicability and implementation of how to achieve the low level security control baseline defined in NIST SP 800-53B Rev. 5 document.

This modelled startup is an actual project that intends to develop an application and infrastructure that offer services similar to a startup called GoworkaBit, in which companies can post job offers, and registered users can apply for them.

The Author aims to find the optimal IaaS platform and implement Blue Teaming<sup>1</sup> solutions to achieve the NIST SP 800-53 Rev. 5 low level security baseline for the selected controls. The compliance scope contains the IaaS platform and connected services like containers, virtual machines, virtual networks, database and domain name

---

<sup>1</sup> The group responsible for defending an enterprise's use of information systems by maintaining its security posture against a group of mock attackers [30].

hosting. At the end of the analysis, compliance is measured with automated tools and in accordance with NIST SP 800-53A Revision 5 document.

## **1.2. Scope and limitations**

1. This thesis focuses on implementing security controls to a cloud-based infrastructure (IaaS) in accordance with the NIST SP 800-53 Rev. 5 standard.
2. The modeled IT environment will be similar, but simplified, to an Estonian startup called GoWorkaBit. Overall, the model could be adapted to most startup environments whose infrastructure utilising cloud computing solutions.
3. The startup model will be an already defined IT environment, and the thesis will not concentrate on how such an infrastructure and mobile application could be developed.
4. The scope of the thesis is limited to NIST SP 800-53 low security control baselines. A newly established company with a limited infrastructure does not require the same level of cyber security compliance as a multinational technological corporation. Moderate or high levels of cyber security compliance may include technologies that this model does not require at this level. There would be a significant increase in cost, but there would be no significant increase in cyber security.
5. Due to similar circumstances, control enhancements are also out of the thesis's scope.
6. Following the filtering, the controls will be selected based on whether or not they comply with the startup infrastructure model.
7. Tools, technologies, services, or configuration changes implemented into components outside the IaaS platform (like domain name configuration) only use open-source solutions.
8. The thesis will focus on easily searchable blue teaming solutions rather than listing all the available tools and technologies worldwide in the analysis section.
9. Due to the limitations of the thesis length, not all applicability analyses and implementation of solutions can be documented in this paper. The Author aims to introduce the most exciting ones within the paper's length limit.

### **1.3. Methodology**

- The modelled startup environment is developed.
- The Author reads the NIST SP 800-53 standard and all the other parts of the publication.
- The IaaS platform selection begins. In selecting the platform, the level of support for standard compliance is the first consideration.
- The Author combines all the introduced NIST documents and the documentation of the IaaS into a Microsoft excel worksheet where the selected controls will be marked.
- The worksheet is filtered into a low security control baseline, and then the selection of the relevant controls starts in accordance with the limitations.
- The selected IaaS platform built-in solutions like rules, policies, and initiatives will be developed and implemented into the cloud-based infrastructure environment.
- Tools, technologies, services, or configuration changes will be incorporated into the Non-IaaS infrastructure according to the selected controls, which will be introduced in two examples.
- The implementations will be analysed by automated tools to see if they meet the selected NIST SP 800-53 Rev. 5 controls.
- The noncompliant controls will be revised, and solutions for compliance will be developed.
- A conclusion will be written that can be used for further research.

## **2. Background**

Before selecting and implementing the applicable controls, it is necessary to understand the purpose and structure of the NIST SP 800-53 Revision 5 standard and the modelled startup infrastructure.

### **2.1. Overview of the NIST SP 800-53 Rev. 5 standard.**

In response to the rapid development of the technological capabilities of national adversaries, the U.S. Department of Commerce and the National Institute of Standards in Technology (NIST) developed NIST SP 800-53 as a security compliance standard. The document contains controls recommended by the Information Technology Laboratory (ITL). A variety of privacy and security controls are provided to protect against a variety of threats. It is widely used by government agencies, critical infrastructure operators, and private sector organisations to protect sensitive information and systems from threats such as cyber attacks, data breaches, and unauthorised access.

The latest version of the standard, Revision 5, was released in 2020 and builds upon previous versions by incorporating new and emerging threats, technologies, and best practices in cybersecurity. It is organised into four major parts: security and privacy controls, control families, control enhancements, and control baselines.

One of the main benefits of NIST SP 800-53 Revision 5 is its flexibility. The standard provides a baseline set of security controls, but it also allows organisations to tailor the controls to their specific needs and risks. This allows organisations to implement a risk management program that is tailored to their unique environment and needs.

The security and privacy controls section defines a comprehensive set of control objectives and controls that organisations can use to protect their information systems and data. These controls are organised into families, each addressing a specific aspect of cybersecurity such as access control, incident response, and system and communications protection. The control families section provides additional guidance and requirements for implementing and managing these controls, including a detailed assessment of the security risks and impacts associated with each control.



The control enhancements section provides additional guidance on how to customise and strengthen the controls to meet the specific needs and risks of an organisation. It includes a set of optional enhancements that organisations can choose to implement based on their risk profile and the sensitivity of the information and systems they are protecting.

Finally, the control baselines section defines a set of minimum controls that organisations must implement based on their risk level and the impact of a security breach. It includes three baselines: low, moderate, and high, with each one increasing in the number and strength of the required controls.

Another significant update in Revision 5 is the inclusion of controls specifically designed for cloud computing environments. These controls address the unique security challenges posed by cloud computing, such as the shared responsibility model and the use of third-party providers.

Overall, NIST SP 800-53 Revision 5 is a comprehensive and flexible standard that provides organisations with the guidance and requirements needed to protect their information systems and data from a wide range of threats. By following the guidelines and requirements outlined in the standard, organisations can ensure that their cybersecurity posture is strong and effective, helping to safeguard their assets and operations [4].

### **2.1.1. Supporting documents**

NIST SP 800-53 Revision 5 is a document that outlines security and privacy controls for federal information systems and organisations. It provides recommendations for protecting the confidentiality, integrity, and availability of information and information systems, including cyber security threats and vulnerabilities. Supporting documents for NIST SP 800-53 Revision 5 include NIST SP 800-53A, which provides guidance on assessing and testing the security controls in federal information systems, and NIST SP 800-53B, which provides guidelines on selecting and implementing security controls. These supporting documents work in conjunction with NIST SP 800-53 Revision 5 to provide a comprehensive set of guidelines for ensuring security and privacy compliance.

All of these documents have Supplemental Materials like spreadsheets for more accessible control selection, mappings which help to find the differences between two

revisions and includes a mapping to other standards and best practices, such as the Cybersecurity Framework and the ISO 27001 standard.

SP 800-53 Rev. 5 main documents:

- **SP 800-53 Rev.5:** This is the document's main body where One can find the detailed specification of controls and their enhancements under control families [5].
- **SP 800-53A Rev.5:** This document is made for auditors to help the audit process in NIST SP 800-53 Rev. 5 compliance assessment. Each control's assessment is detailed step by step [6].
- **SP 800-53B Rev.5:** This document categorises the controls into three security control baselines – low, moderate and high. One control can be a part of all three security baseline levels [7].

### **2.1.2. Families and control structure**

Control families are similar to the main cyber security areas that must be covered (for example, Incident Response, System and Communications Protection). Controls can be defined as a list of tasks for a specific technology, workflow, business logic or governmental requirement. It can be physical, logical, environmental or data type.

Under the families, there is a list of base controls covering all possible scenarios One should consider in the scope of hardening cyber security. The base controls may include enhancements that are used in systems and environments that require a higher level of protection than that provided by the base controls.

The NIST SP 800-53 Rev. 5 standard contains 20 control families and 1189 controls [5].

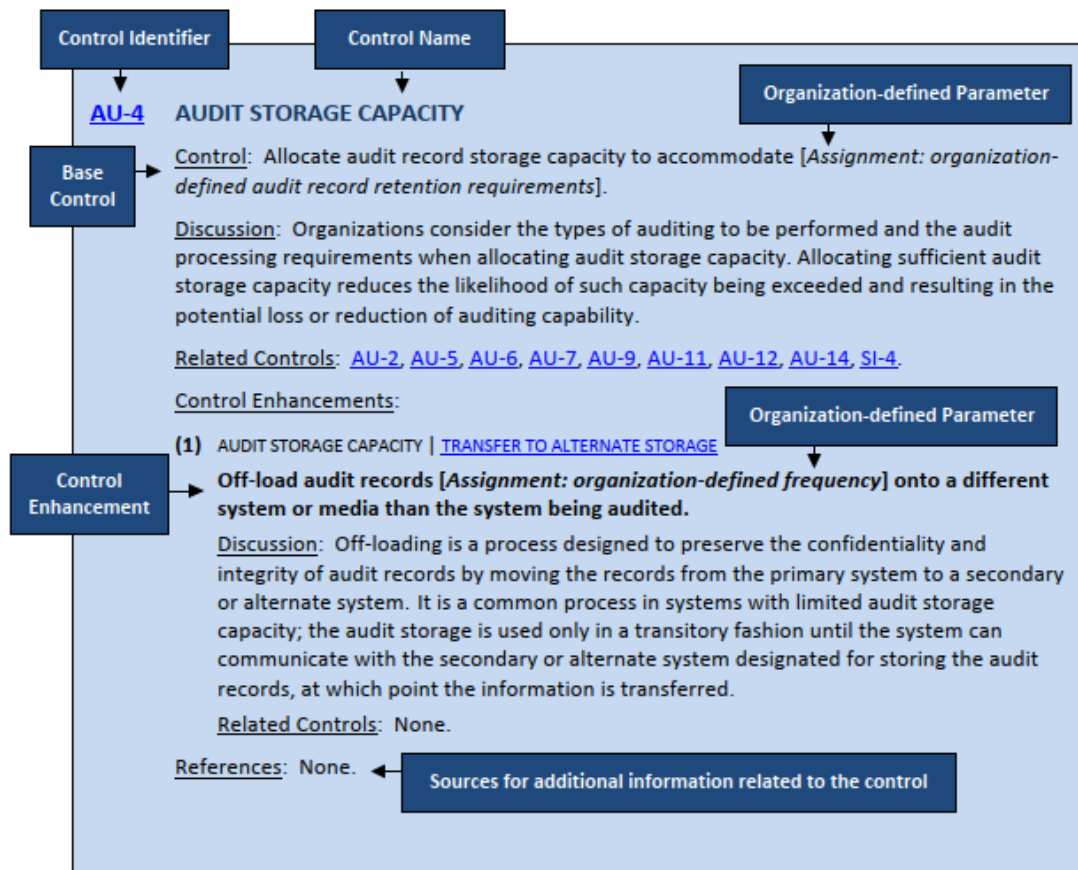


Figure 1. Control structure [8]

### 2.1.3. Reasons for choosing the standard

The NIST SP 800-53 Revision 5 standard was selected to satisfy the Hungarian regulatory compliance requirements for information systems that process personal data. In Hungary, there is a decree which contains a major part of the standard translated. It is called 41/2015. (VII. 15.) BM decree. Modelled infrastructure will be run by a Hungarian startup and will process personal data. Complying with the requirements of IaaS platforms is simpler than complying with the decree .

In addition, the standard is widely used, and Revision 5 includes cloud computing controls, in contrast to older versions and most cyber security standards that protect entire organisations and infrastructures.

Lastly, in the author's subjective opinion, NIST SP 800-53 is much more detailed than other cyber security standards.

## **2.2. Overview of the startup model**

Microsoft Azure is a cloud computing platform that offers a range of services and tools for building, deploying, and managing applications and services. It is designed to help organisations of all sizes, from small startups to large enterprises, take advantage of the benefits of cloud computing.

Azure provides a range of services including computing, storage, networking, analytics, and machine learning, which can be used individually or combined to create customised solutions that meet the specific needs of an organisation. One of the key benefits of Azure is its flexibility, which allows organisations to scale up or down as their needs change, and pay only for the resources they use.

In addition to its wide range of services and global presence, Azure is also known for its security and reliability. The platform is designed to meet the highest security standards and undergoes regular security assessments to ensure that it is meeting these standards. It includes a range of security features and controls, such as data encryption, authentication, and access control, to help protect customer data and applications. Additionally, Azure is compliant with a number of industry and regulatory standards, making it a good choice for organisations with specific security and compliance requirements. The platform is built on a network of data centers that are designed to be highly available and redundant, and it includes a range of security features to protect data and applications.

Overall, Microsoft Azure is a powerful and flexible cloud computing platform that offers a range of services and tools for building, deploying, and managing applications and services. Its reliability, security, and integration with other Microsoft technologies make it a popular choice for organisations of all sizes [9].

### **2.2.1. Selection of the IaaS platform**

The Author narrowed down the selection of IaaS providers to AWS, Microsoft Azure, and Google Cloud. Cyber security compliance with security standards was one of the most significant considerations in the selection process:

- **AWS:** According to Amazon's documentation, its IaaS solution only supports NIST SP 800-53 Rev. 4, and its customers are responsible for developing most controls [10].
- **Google Cloud:** Google Cloud complies with the standard in scope but has no document describing how it adheres to the controls [11].
- **Microsoft Azure:** Microsoft Azure supports Rev. 5 and provides detailed instructions on implementing each control by adding Azure Policies to the IaaS environment [12].

According to the research, Microsoft Azure provides the most support and documentation regarding compliance with the standard.

**Access Control**

**Policy and Procedures**

ID: NIST SP 800-53 Rev. 5 AC-1 Ownership: Shared

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Develop access control policies and procedures</a>	CMA_0144 - Develop access control policies and procedures	Manual, Disabled	1.1.0
<a href="#">Enforce mandatory and discretionary access control policies</a>	CMA_0246 - Enforce mandatory and discretionary access control policies	Manual, Disabled	1.1.0
<a href="#">Govern policies and procedures</a>	CMA_0292 - Govern policies and procedures	Manual, Disabled	1.1.0
<a href="#">Review access control policies and procedures</a>	CMA_0457 - Review access control policies and procedures	Manual, Disabled	1.1.0

Figure 2. Detailed support of controls [12]

## 2.2.2. Components of the infrastructure

### 1. Web server

The virtual machine platform in Microsoft Azure hosts a virtual web server called TestVM. Linux is its operating system, and Ubuntu is its distribution using a public IP. A second purpose of the server is to test cyber security tools, technologies, software, and

services for compliance with security controls.

## **2. Docker**

Using the Docker service, TestVM runs both the backend and reverse proxy through separate Docker containers.

## **3. Quarkus**

The backend is implemented in Quarkus lightweight framework microservice architecture. Its primary purpose is to handle HTTP requests and send data to the NoSQL database. The backend runs on a Docker container on the TestVM virtual web server.

## **4. Azure Cosmos DB**

Users' data is stored in Azure Cosmos DB. The backend data is stored in a NoSQL database in the form of JSON files. Users' information is stored in Azure Cosmos DB. The backend data is stored in a NoSQL database in the form of JSON files.

## **5. Envoy proxy**

The envoy proxy functions as a reverse proxy. When the Android application sends HTTPS requests to the proxy, the proxy terminates the SSL and communicates with the backend using plain HTTP. Login and registration data are provided as Google identity tokens, authenticated from the database using an email address.

## **6. Domain hosting platform**

The domain names were registered through Cloudflare. In order to conceal the backend IPV4 address, Cloudflare proxies requests from clients to the model's cloud infrastructure. In the proxy before the backend, HTTPS certificates were provided by the platform. The model can be protected from DDoS attacks and handle large batches of requests from the same IP address.

## **7. Kotlin**

The android application is written in Android Studio with kotlin programming language, and its primary purpose is registration and login to the model via google authentication.

### **2.2.3. Overview of the Azure IaaS platform**

Through Microsoft's global network of datacenters, Microsoft Azure provides developers and IT professionals with a platform for building, deploying and managing cloud-based applications [13]. For developing the model, the following services have been used:

#### **1. Compute**

The Azure platform enables One to make and manage virtual machines with several OS possibilities. The model uses the Virtual Machine resource with a static IP address which provides the Linux OS.

#### **2. Networking**

The Microsoft Azure cloud platform offers tools that can be used to connect the resources inside the cloud or cloud servers to on-premise data centers. The model uses the Virtual Network, Virtual Network interface, and Network Security Group resources to communicate with other infrastructure elements.

#### **3. Storage**

Cloud storage enables data to be stored in the cloud, which can be accessed from anywhere at any time. The model uses the Virtual Disk Storage resource and provides the TestVM's storage.

#### **4. Databases**

Azure provides reliable relational and non-relational database instances under the database domain. The model uses Azure Cosmos DB serving as the user and job database.

#### **5. Security + Identity**

The model uses the Key Vault resource, where we store CA-signed certificates. Also, an SSH key is registered to the platform for connecting the TestVM securely.

Filter for any field... Type equals all X Location equals all X Add filter

Showing 1 to 9 of 9 records.  Show hidden types  List view










<input type="checkbox"/> Name ↑↓	Type ↑↓	Location ↑↓	
<input type="checkbox"/>  cosmosdb-jajob	Azure Cosmos DB account	Switzerland North	***
<input type="checkbox"/>  EnvoyConfigs	Key vault	UK South	***
<input type="checkbox"/>  TestVM	Virtual machine	UK South	***
<input type="checkbox"/>  TestVM-ip	Public IP address	UK South	***
<input type="checkbox"/>  TestVM-nsg	Network security group	UK South	***
<input type="checkbox"/>  testvm921	Network Interface	UK South	***
<input type="checkbox"/>  TestVM_disk1_60a2be862bdb4bb5b0270a6da80ddf9e	Disk	UK South	***
<input type="checkbox"/>  TestVM_group-vnet	Virtual network	UK South	***
<input type="checkbox"/>  TestVM_key	SSH key	UK South	***

Figure 3. Microsoft Azure Platform TestVM\_group



### 3. Control selection

#### 3.1. Selection methodology of applicable controls

The main goal is to list all the controls and order them by the security control baseline. For this task, the Author has used the official spreadsheets provided by NIST under the Supplemental Materials section of the webpage [5].

Control ID	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
AC-2	Account Management	a. Define and document the types of accounts allowed and specifically prohibited for use within the system; b. Assign account managers; c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership; d. Specify: 1. Authorized users of the system; 2. Group and role membership; and 3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account; e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts; f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria]; g. Monitor the use of accounts; h. Notify account managers and [Assignment: organization-defined personnel or roles] within: 1. [Assignment: organization-defined time period] when accounts are no longer required; 2. [Assignment: organization-defined time period] when users are terminated or transferred; and 3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual; i. Authorize access to the system based on: 1. A valid access authorization; 2. Intended system usage; and 3. [Assignment: organization-defined attributes (as required)]; j. Review accounts for compliance with account management requirements [Assignment: organization-defined policy, procedures, prerequisites, and criteria].	Examples of system account types include individual, shared, group, system, guest, anonymous, emergency, developer, temporary, and service. Identification of authorized system users and the specification of access privileges reflect the requirements in other controls in the security plan. Users requiring administrative privileges on system accounts receive additional scrutiny by organizational personnel responsible for approving such accounts and privileged access, including system owner, mission or business owner, senior agency information security officer, or senior agency official for privacy. Types of accounts that organizations may wish to prohibit due to increased risk include shared, group, emergency, anonymous, temporary, and guest accounts. Where access involves personally identifiable information, security programs collaborate with the senior agency official for privacy to establish the specific conditions for group and role membership; specify authorized users, group and role membership, and access authorizations for each account; and create, adjust, or remove system accounts in accordance with organizational policies. Policies can include such information as account expiration dates or other factors that trigger the disabling of accounts. Organizations may choose to define access privileges or other attributes by account, type of account, or a combination of the two. Examples of other attributes required for authorizing access include restrictions on time of day, day of week, and point of origin. In defining other system account attributes, organizations consider system-related requirements and mission/business requirements. Failure to consider these factors could affect system availability. Temporary and emergency accounts are intended for short-term use. Organizations establish temporary accounts as part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be used for long-term access.	AC-3, ACS-5, AC-6, AC-17, AC-18, AC-20, AC-24, AU-2, AU-12, CM-5, IA-2, IA-4, IA-5, IA-8, MA-3, MA-5, PE-2, PL-4, PS-2, PS-4, PS-5, PS-7, PT-2, PT-3, SC-7, SC-12, SC-13, SC-37.
AC-2(1)	Account Management   Automated System Account Management	Support the management of system accounts using [Assignment: organization-defined automated mechanisms].	Automated system account management includes using automated mechanisms to create, enable, modify, disable, and remove accounts; notify account managers when an account is created, enabled, modified, disabled, or removed, or when users are terminated or transferred; monitor system account usage; and report atypical system account usage. Automated mechanisms can include internal system functions and email, telephonic, and	None.

Figure 4. Control Catalog (spreadsheet) (xls) for the SP 800-53 Rev. 5 standard

This table does not contain the security control baseline levels, so the Author merged the official 800-53 Rev. 5 spreadsheet with the official SP 800-53B Rev. 5 Control Baselines spreadsheet, which contains the needed data. [7].

	A	B	C	D	E	F	G	H
	Sort-As	Control Identifier	Control (or Control Enhancement) Name	Withdrawn	Privacy Baseline	Security Control Baseline - Low	Security Control Baseline - Moderate	Security Control Baseline - High
2	AC-01-00	AC-1	Policy and Procedures		X	X	X	X
3	AC-02-00	AC-2	Account Management			X	X	X
4	AC-02-01	AC-2(1)	Account Management   Automated System Account Management				X	X
5	AC-02-02	AC-2(2)	Account Management   Automated Temporary and Emergency Account Management				X	X
6	AC-02-03	AC-2(3)	Account Management   Disable Accounts				X	X
7	AC-02-04	AC-2(4)	Account Management   Automated Audit Actions				X	X
8	AC-02-05	AC-2(5)	Account Management   Inactivity Logout				X	X
9	AC-02-06	AC-2(6)	Account Management   Dynamic Privilege Management					
10	AC-02-07	AC-2(7)	Account Management   Privileged User Accounts					
			Account Management   Dynamic					

Figure 5. Control Baselines spreadsheet (xls) for SP 800-53B Rev. 5

The Author selected the controls based on the scope and limitations section and used color coding where the Green rows represent the selected controls.

Control (or Control Enhancement) Name	Control Identifier	FAMILY	Security Control Baseline - Low	Security Control Baseline - Moderate	Security Control Baseline - High	Color Index
Policy and Procedures	AC-1	Access Control	x	x	x	Light Red
Account Management	AC-2	Access Control	x	x	x	Green
Access Enforcement	AC-3	Access Control	x	x	x	Green
Unsuccessful Logon Attempts	AC-7	Access Control	x	x	x	Green
Permitted Actions Without Identification or Authentication	AC-14	Access Control	x	x	x	Green
Remote Access	AC-17	Access Control	x	x	x	Green

Figure 6. Selected Controls

After the end of the selection process, 51 controls were selected, which are listed in Error! Reference source not found. section due to the length of the table [14].

### 3.2. Merging Azure policies with the selected controls

For each control, there is a list of Azure policies which can be assigned to the infrastructure introduced in section 2.2.1 Selection of the IaaS platform. These policies are responsible for the modelled infrastructure's compliance analysis and system configuration changes.

The author has created a Microsoft Excel spreadsheet that contains all controls, control families, and assigned policies based on the official Azure manual [15] in order to provide a better understanding of the Azure policy architecture and provide the possibility of control filtering. Then color-coded the selected controls in the same way as in the selection methodology.

	B	C	D	E	F	H
1	NIST Assigned Azure Controls 2	Family	Description	Effect(s)	Version	
10	<a href="#">ID: NIST SP 800-53 Rev. 5 AC-2 Ownership: Shared</a>	Access Control				
	<a href="#">A maximum of 3 owners should be designated for your subscription</a>	Access Control	It is recommended to designate up to 3 subscription owners in order to reduce the potential for breach by a compromised owner.	AuditIfNotExists, Disabled	<a href="#">3.0.0</a>	
11	<a href="#">An Azure Active Directory administrator should be provisioned for SQL servers</a>	Access Control	Audit provisioning of an Azure Active Directory administrator for your SQL server to enable Azure AD authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services	AuditIfNotExists, Disabled	<a href="#">1.0.0</a>	
12	<a href="#">App Service apps should use managed identity</a>	Access Control	Use a managed identity for enhanced authentication security	AuditIfNotExists, Disabled	<a href="#">3.0.0</a>	
13	<a href="#">Assign account managers</a>	Access Control	CMA_0015 - Assign account managers	Manual, Disabled	<a href="#">1.1.0</a>	
14	<a href="#">Audit usage of custom RBAC rules</a>	Access Control	Audit built-in roles such as 'Owner, Contributor, Reader' instead of custom RBAC roles, which are error prone. Using custom roles is treated as an exception and requires a rigorous review and threat modeling	Audit, Disabled	<a href="#">1.0.0</a>	
15	<a href="#">Audit user account status</a>	Access Control	CMA_0020 - Audit user account status	Manual, Disabled	<a href="#">1.1.0</a>	
16	<a href="#">Cognitive Services accounts should have local authentication methods disabled</a>	Access Control	<a href="#">Disabling local authentication methods improves security by ensuring that Cognitive Services accounts require Azure</a>	Audit, Deny, Disabled	<a href="#">1.0.0</a>	

Figure 7. Selected controls with azure policies

Hereinafter this spreadsheet will be used as the primary guide in implementing Azure policies into the modelled infrastructure environment [14].

## 4. Applicability Analysis and Implementation

There are two methodologies used in the applicability analysis and implementation process. First, the Azure cloud-based infrastructure must be hardened until complete compliance with the selected controls is achieved. Second, tools, technologies, services, or configuration changes may be used to harden infrastructure components which are located outside of the IaaS platform .

Because of the limitations of the paper, there will be two controls will be analysed in detail: System and Communications Protection: SC-5 Denial-of-service Protection Control and System and Communications Protection: SC-7 Boundary Protection Control. These two controls are applicable in both cases and differences in control implementation between IaaS and external resources can be introduced.

### **1. System and Communications Protection: SC-5 Denial-of-service Protection Control:**

The NIST SP 800-53 Revision 5 SC-5 Denial-of-service Protection control is a critical cybersecurity measure that aims to protect against threats that may disrupt the availability of a system or service. Denial-of-service attacks can come from external sources, such as a malicious actor attempting to overwhelm a system with traffic, or internal causes such as insufficient capacity or bandwidth to support organisational needs. These attacks can occur on various network protocols, including IPv4 and IPv6, making it important for organisations to have robust protection in place. The goal of the SC-5 control is to prevent or mitigate the impact of these types of events, ensuring that critical systems and services remain available and operational. This is accomplished through a variety of security measures and controls, including network segmentation, traffic filtering, and rate limiting [5].

### **2. System and Communications Protection: SC-7 Boundary Protection Control:**

NIST SP 800-53 Revision 5 SC-7 Boundary Protection control is a cybersecurity measure that helps organisations protect the boundaries of their systems and networks from external threats. This control ensures that the organisation has implemented the necessary

security controls to prevent unauthorised access or tampering with their systems and networks from external sources. This can include measures such as firewalls, intrusion detection and prevention systems, and network segmentation. By implementing these controls, an organisation can reduce the risk of cyber attacks and protect sensitive data from being accessed or stolen by external parties. Additionally, SC-7 Boundary Protection control emphasises the importance of monitoring and detecting any unauthorised access or attempted breaches at the network boundary and taking appropriate actions to prevent or mitigate the risk of data loss or compromise [5].

## **4.1. Azure infrastructure compliance**

To address these needs, Microsoft has created a comprehensive Compliance Ecosystem for Azure. This ecosystem includes a range of features and services that enable organisations to ensure the security, privacy, and compliance of their cloud-based applications and data. For example, Azure provides support for industry-specific compliance standards such as HIPAA, PCI DSS and NIST SP 800-53 as well as regional frameworks like GDPR, the California Consumer Privacy Act [16]. The Microsoft Compliance Ecosystem contains three main services: the Azure Policy Service, the Microsoft Defender for Cloud Service and the Microsoft Sentinel Service.

- Azure Policy service is responsible for auditing policies and initiatives to determine if they are compliant or not.
- Microsoft Defender for Cloud Service is responsible for managing the firewalls, measuring the overall security posture based on connected services and enforcing rules for regulatory compliance.
- Azure Sentinel Service collects and analyses logs and data from the input determined by the administrator. It can enforce system changes or act like an IDS or IPS based on its configuration. Finally, it supports regulatory compliance analysis, can generate reports and enforce configuration changes based on security posture logs.

The three main services are intertwined/overlapped into each other, and their overall

configuration provides Microsoft Azure's Regulatory Compliance Ecosystem .

#### **4.1.1. Azure Policy Service**

##### **Service Description:**

Azure Policy is a service provided by Microsoft Azure that allows administrators to create, assign, and manage policies. These policies define rules and actions that can be enforced on resources within the Azure platform. This helps ensure that resources are compliant with corporate standards and industry regulations and helps prevent unwanted or unexpected changes to resources [17].

There are two types of policies that can be created and enforced with Azure Policy. One type is a policy definition, which specifies the rules and actions that should be taken when a policy is evaluated. Another type is a policy initiative, which is a collection of policy definitions that are grouped together to address a specific compliance requirement or business need.

Policy definitions can be written in JSON or Azure Resource Manager (ARM) templates and can be used to enforce a variety of rules and actions on Azure resources. For example, a policy definition could be used to ensure that all virtual machines are configured with a specific type of operating system, or to prevent the creation of public IP addresses on virtual machines.

Policy initiatives can be used to enforce multiple policies at once and can be assigned to specific resource groups or subscriptions. This allows administrators to easily manage and enforce compliance including the NIST SP 800-53 Rev. 5 initiative across a large number of resources.

Finally, the Policy Insights feature allows administrators to see which resources are noncompliant with policies, and to view the history of policy evaluation for a given resource.

##### **Implementation:**

There are two major subpages on the Azure Policy page:

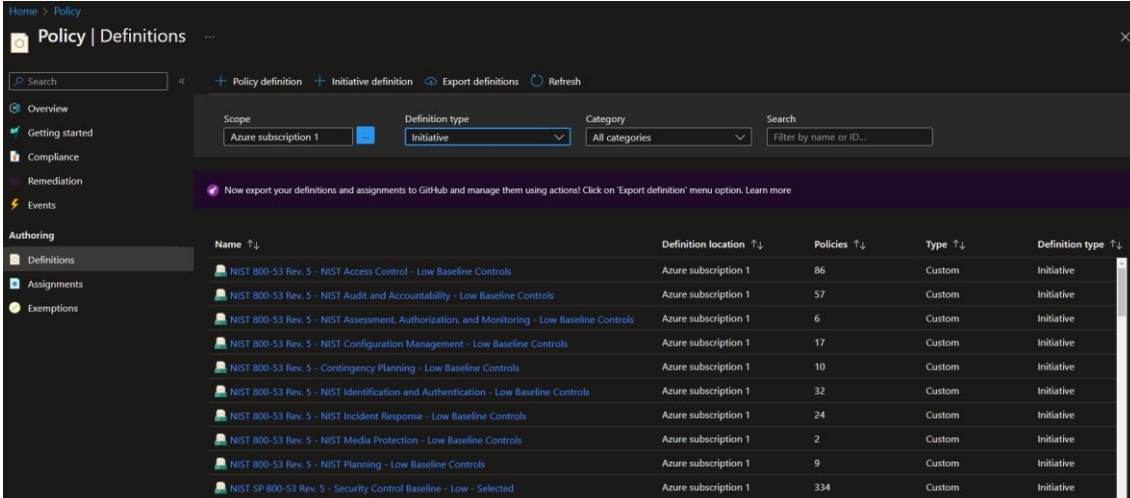
- On the "Compliance" page, the administrator is able to examine the level of

compliance with the policies and initiatives assigned to him.

- On the "Definition" page, One can assign predefined policies and initiatives, or define custom policies and initiatives.

Three best practices have been applied to this project. As a first step, the Author has assigned the predefined complete NIST SP 800-53 Rev. 5 initiative. Then duplicated the initiative, configured a version containing only the selected controls from the selected controls spreadsheet page, and named the initiative "NIST SP 800-53 Rev. 5 - Security Control Baseline - Low – Selected". Lastly, the Author has defined two custom initiatives containing policies for the SC-5 and SC-7 controls based on the "Azure NIST initiative with MS" spreadsheet.

By using this approach, the Author is able to identify the differences and gaps that must be addressed in order to achieve selected and full compliance. Figure 8 shows the compliance level before the Author made any changes to Azure Portal.



The screenshot shows the 'Policy | Definitions' interface in the Azure portal. It features a search bar, navigation tabs for 'Policy definition', 'Initiative definition', and 'Export definitions', and a filter section for 'Scope' (set to 'Azure subscription 1'), 'Definition type' (set to 'Initiative'), and 'Category' (set to 'All categories'). A table below lists various policy definitions with columns for Name, Definition location, Policies, Type, and Definition type.

Name	Definition location	Policies	Type	Definition type
NIST 800-53 Rev. 5 - NIST Access Control - Low Baseline Controls	Azure subscription 1	86	Custom	Initiative
NIST 800-53 Rev. 5 - NIST Audit and Accountability - Low Baseline Controls	Azure subscription 1	57	Custom	Initiative
NIST 800-53 Rev. 5 - NIST Assessment, Authorization, and Monitoring - Low Baseline Controls	Azure subscription 1	6	Custom	Initiative
NIST 800-53 Rev. 5 - NIST Configuration Management - Low Baseline Controls	Azure subscription 1	17	Custom	Initiative
NIST 800-53 Rev. 5 - Contingency Planning - Low Baseline Controls	Azure subscription 1	10	Custom	Initiative
NIST 800-53 Rev. 5 - NIST Identification and Authentication - Low Baseline Controls	Azure subscription 1	32	Custom	Initiative
NIST 800-53 Rev. 5 - NIST Incident Response - Low Baseline Controls	Azure subscription 1	24	Custom	Initiative
NIST 800-53 Rev. 5 - NIST Media Protection - Low Baseline Controls	Azure subscription 1	2	Custom	Initiative
NIST 800-53 Rev. 5 - NIST Planning - Low Baseline Controls	Azure subscription 1	9	Custom	Initiative
NIST SP 800-53 Rev. 5 - Security Control Baseline - Low - Selected	Azure subscription 1	334	Custom	Initiative

Figure 8. Policy | Definitions

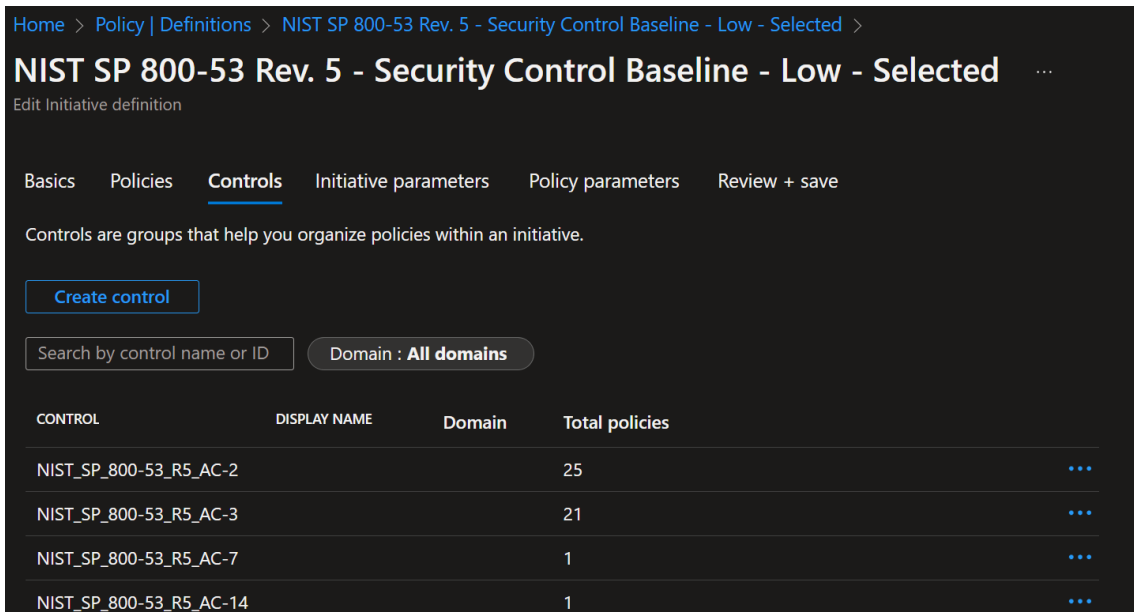


Figure 9. Initiative of selected controls

In Figure 9, it can be seen that the SC-5 control compliance has been achieved. This is due to the fact that the Author has installed the resources utilised in the platform with the default configuration. Configurations such as these have a level of security that complies with the standard.

SC-7 controls are partially compliant by default. The table 1 shows that 6 out of 43 policies were noncompliant. The noncompliant policies were the following:

Name	Noncompliant Resources	Total resources
Storage accounts should use private link	2	2
Storage accounts should restrict network access using virtual network rules	1	2
Storage accounts should restrict network access	1	2
CosmosDB accounts should use private link	1	1



Container registries should not allow unrestricted network access	1	1
Container registries should use private link	1	1

Table 1. SC-7 noncompliant policies

#### 4.1.2. Microsoft Defender for Cloud

##### Service Description:

Microsoft Defender for Cloud is a security service offered by Microsoft that helps organisations protect their cloud-based environments from cyber threats. It is designed to protect against a wide range of threats, including malware, ransomware, and phishing attacks, and is integrated with various Microsoft cloud services [18].

One of the key features of Microsoft Defender for Cloud is its ability to provide real-time protection against threats. It uses advanced machine learning algorithms to detect and block threats, ensuring that organisations are protected against the latest threats as they emerge.

In addition to its real-time protection and comprehensive visibility capabilities, Microsoft Defender for Cloud also offers a number of other key features that help organisations better protect their cloud-based environments. These include:

- **Security Posture:** Microsoft Defender for Cloud Security Posture Management is a service that helps organisations secure their cloud environments by providing continuous monitoring and assessment of their cloud infrastructure. This service utilises machine learning and artificial intelligence to detect potential security threats and vulnerabilities, and provides recommendations for remediation.
- **Regulatory Compliance:** Microsoft Defender for Cloud helps organisations ensure that they are compliant with various industry and regulatory standards, including NIST SP 800-53.

- **Firewall Manager:** Microsoft Defender for Cloud Firewall Manager is a service that helps organisations secure their cloud environments by providing a cloud-native firewall solutions. This service enables organisations to create and enforce security rules to protect their cloud resources and applications from external threats.

### **Implementation:**

The selected controls have been implemented using Microsoft Defender for Cloud Regulatory Compliance. One can assign policies and initiatives defined in Azure Policy Service, including custom initiatives.

The link shown in Figure 10 can be used to manage compliance policies and to add new ones. The Author has assigned the initiatives defined in Azure Policy Service to the platform.



Figure 10. Microsoft Defender for Cloud Regulatory compliance

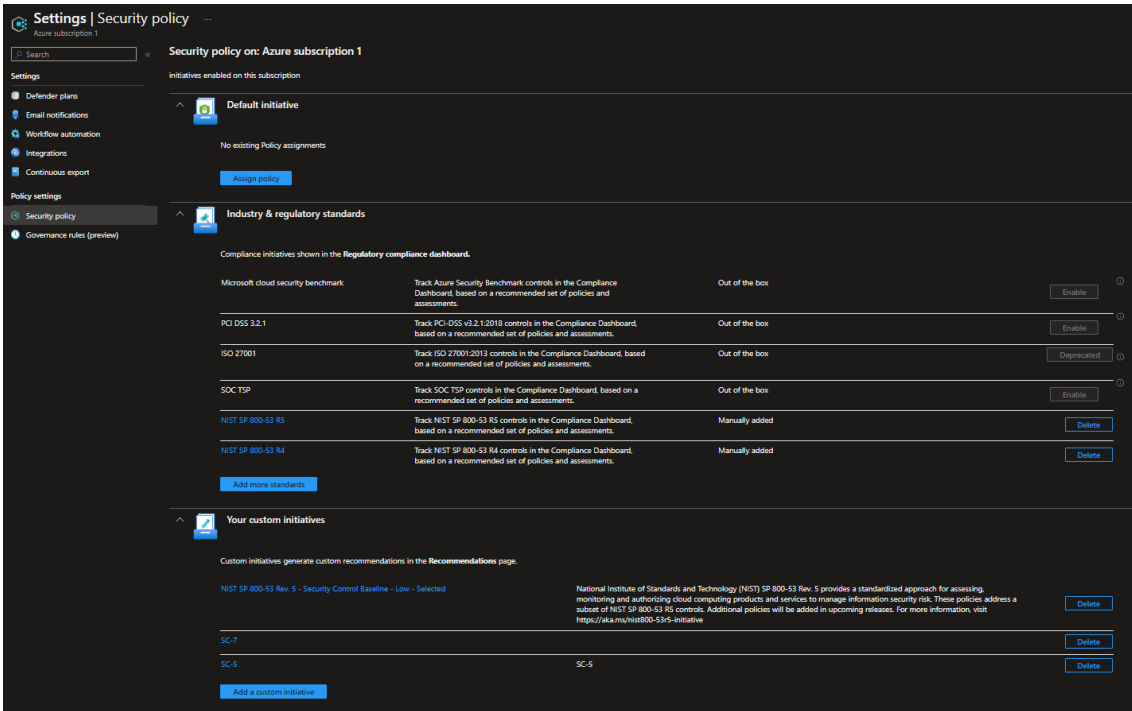


Figure 11. Applied initiatives

Once Azure has completed the implementation of selected initiatives and policies, One can examine the controls within the assigned standard. Whenever a noncompliance is identified, the Author is able to assign automated changes ("Quick fix!") to the system shown in figure 12.

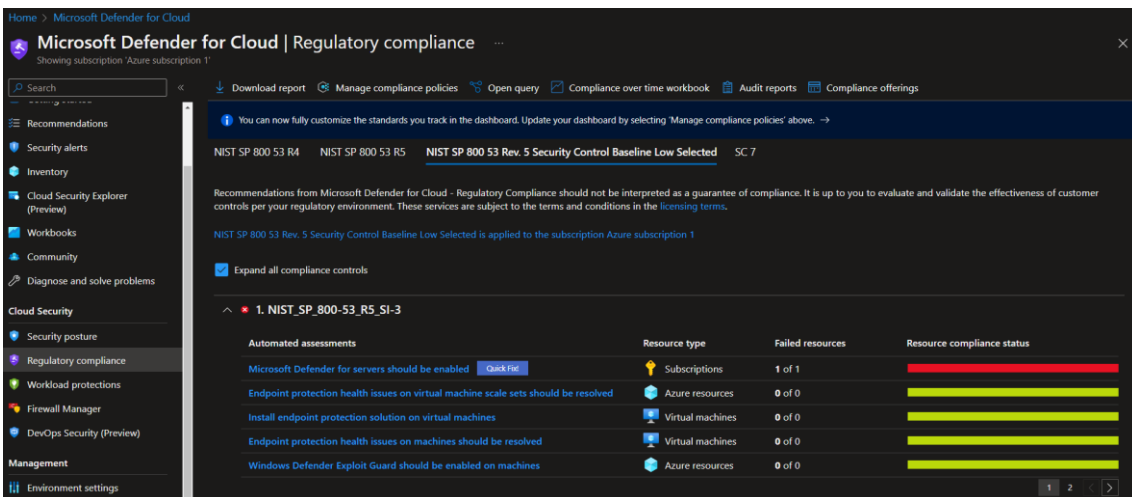


Figure 12. Configuration change deployment

According to SC-5's control, no configuration change recommendations were identified, but non-applicability status were defined. While SC-7 has 6 recommendations aligned with Azure Policy's non-compliances.

### **4.1.3. Microsoft Sentinel Service**

#### **Service Description:**

Microsoft Sentinel is a cloud-native security information and event management (SIEM) platform that helps organisations detect, prevent, and respond to threats. It uses advanced machine learning algorithms to analyse large amounts of data from multiple sources, including security logs, applications, and devices, to identify unusual activity and potential security breaches [19].

Furthermore, Microsoft Sentinel is able to provide a comprehensive view of an organisation's security posture including compliance with NIST SP 800-53. By collecting and analysing data from a range of sources, it can provide a complete picture of an organisation's security risks, allowing security teams to make informed decisions about how to best protect their systems.

#### **Implementation:**

Following the creation of the service, the Author selected the NIST SP 800-53 solution from "Microsoft Sentinel | Content hub". From this solution, the NISTSP80053workbook has been utilised.

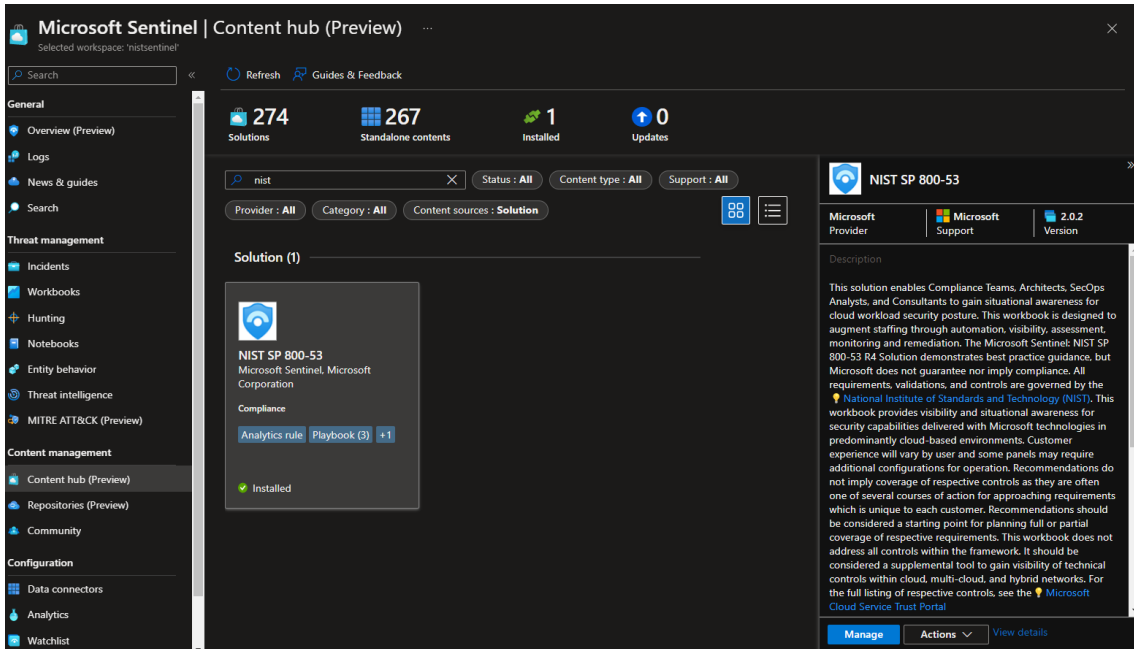


Figure 13. Microsoft Sentinel | Content hub

NISTSP80053workbook provides an opportunity to examine controls under control families and make recommendations for hardening the infrastructure based on logs and data collected from Azure Policy and Microsoft Defender for Cloud.

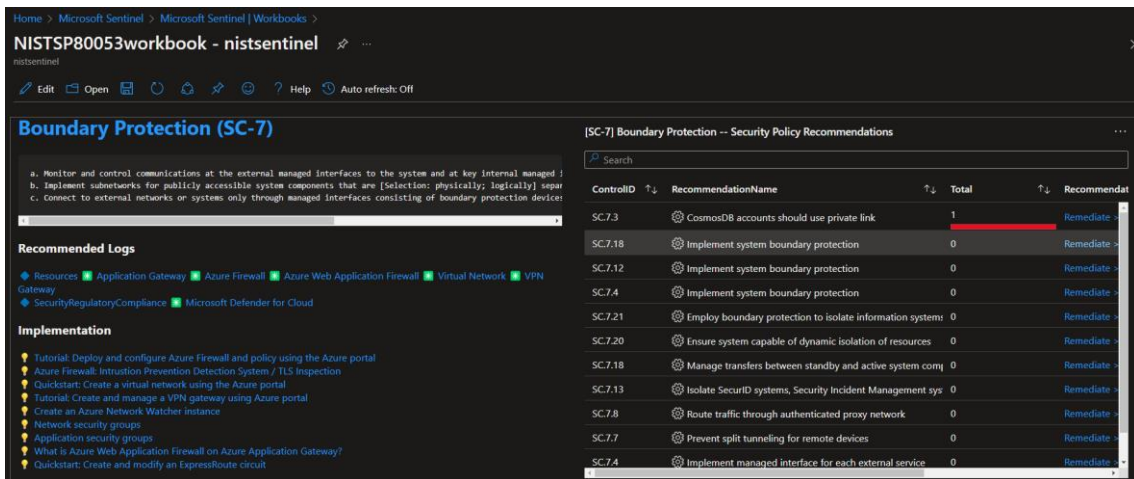


Figure 14. Control overview in Microsoft Sentinel

Further hardening recommendations for Denial of Service Protection (SC-5) control have not been identified. Contrary to this, the collected logs showed failures in the "CosmosDB accounts should use private link" policy under Boundary Protection (SC-7) control.

## **4.2. Non-IaaS component compliance**

Services, technologies, software, hardware, and tools outside the IaaS platform can communicate with the Azure Infrastructure, but they compliance usually cannot be managed by Azure Portal.

Those third-party services which are separated from the portal based on the administrator's decision like Domain Name Hosting or Mobile Application Hosting needs further configuration to fulfill the compliance with the standard. These types of services usually cannot be managed by the Microsoft Compliance Ecosystem and fulfilling compliance with the standard requires further configuration by administrators.

### **4.2.1. Domain Name Hosting**

#### **Description:**

Cloudflare Domain Name Hosting is a service offered by Cloudflare, a leading content delivery network and internet security company. It allows individuals and organisations to register and manage their own domain names, which are used to identify and locate websites on the internet. Another advantage of using Cloudflare Domain Name Hosting is its reliability. The company has a strong track record of uptime and performance, ensuring that users' websites are always available to their visitors. In addition, Cloudflare provides a range of security measures to protect users' domain names and websites from cyber threats, including domain name system (DNS) security, spam and malware protection, and secure socket layer (SSL) encryption. Cloudflare also offers additional features and services such as web hosting, website performance optimisation, and content delivery network services [20].

In order to present compliance with SC-5 and SC-7 controls, the Author registered two Domain Names. The non-protected domain name is jojob.work, while the protected domain name is jojobworks.com. The following sections will introduce a Cloudflare environment with low security, equivalent to a newly registered domain name with default settings.

## 4.2.2. DNS Settings:

Cloudflare DNS Settings offer a number of features to help secure and optimise One's domain's DNS. One of these features is DNSSEC, which helps to protect against DNS spoofing and tampering by adding an extra layer of security to One's DNS records. Another feature is CNAME Flattening, which follows a CNAME to point and return an IP address instead of the CNAME record. Finally, Cloudflare's Email Security feature helps to protect against phishing and spam by scanning incoming emails and blocking any malicious ones. Overall, these features provide an additional level of security and optimisation for One's domain's DNS, helping to ensure that One's website is running smoothly and safely. All of these settings above were disabled in the non-protected domain name [21].

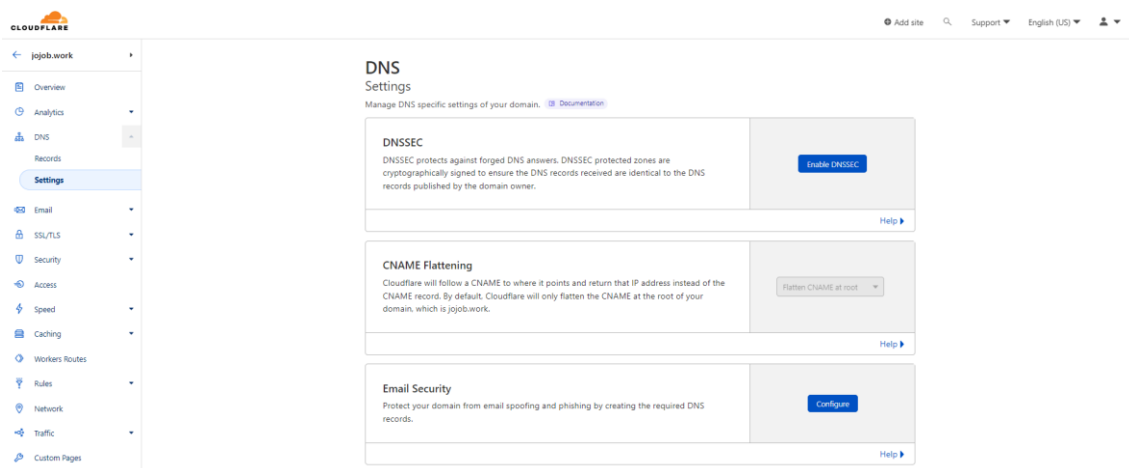


Figure 15. Cloudflare DNS settings

## 4.2.3. SSL/TLS

Cloudflare allows One to select the level of SSL/TLS encryption that should be used on a website. Using Cloudflare's Universal SSL feature, One can provide SSL/TLS encryption for One's website without having to purchase and install a separate SSL certificate. A total of four levels are available: Off, Flexible, Full (strict), and Full

(strict). By default, the domain name SSL/TLS encryption mode has been set to Flexible [22].

## SSL/TLS

Overview [Documentation](#)

The screenshot displays the Cloudflare SSL/TLS settings page. At the top, a green checkmark icon indicates that the SSL/TLS encryption mode is set to 'Flexible'. Below this, a message states 'This setting was last changed a few seconds ago'. A diagram illustrates the traffic flow: a 'Browser' icon connects to a 'Cloudflare' icon (a cloud with a shield), which then connects to an 'Origin Server' icon (a server rack). To the right of the diagram, four radio button options are listed: 'Off (not secure)' (unselected), 'Flexible' (selected), 'Full' (unselected), and 'Full (strict)' (unselected). Each option has a brief description of its encryption scope. Below the options, a link points to 'Learn more about End-to-end encryption with Cloudflare.' A blue button at the bottom of the main panel says 'Create a Configuration Rule to customize these settings by hostname.' At the bottom right of the main panel are links for 'API' and 'Help'. Below the main panel is a section titled 'SSL/TLS Recommender' with a description and a toggle switch that is currently turned off. A 'Help' link is located at the bottom right of this section.

Figure 16. Cloudflare SSL/TLS settings

### 4.2.4. Security Settings

Cloudflare Security Settings provides a variety of security and performance services for websites. One of its key features is the Web Application Firewall (WAF), which provides protection against a range of online threats such as SQL injection attacks and cross-site scripting (XSS). Cloudflare also offers Page Shield, which is designed to prevent abusive traffic from reaching a website and causing issues such as server overload. Additionally, Cloudflare has options to block or challenge suspicious bots that may be trying to access a site. Lastly, Cloudflare provides protection against distributed denial of service (DDoS) attacks, which are attempts to make a website unavailable by overwhelming it with traffic



from multiple sources.

The domain name configured with default settings had no WAF firewall rules, no DDoS protection and had low security level [23].

## 5. Results

The goals set at the beginning of the paper were partially met after the applicability analysis and implementation. However, only a minimum amount of control compliance was not fulfilled the expected outcomes. The noncompliant elements will be revised in further works, and a document will be written addressing the remaining applicability analysis and implementation in order to fulfil the demanded state.

### 5.1. Azure infrastructure compliance results

The compliance with NIST 800-53 Revision 5 standard within the Microsoft Azure Platform achieved an 80% Security Posture score which is considered the primary measurement method of the Azure Compliance Ecosystem. One policy in scope stayed in noncompliant status after executing the recommended Blue Teaming solutions.

The other missing percentage came from control enhancement measurements which cannot be excluded from Microsoft Sentinel's scope.

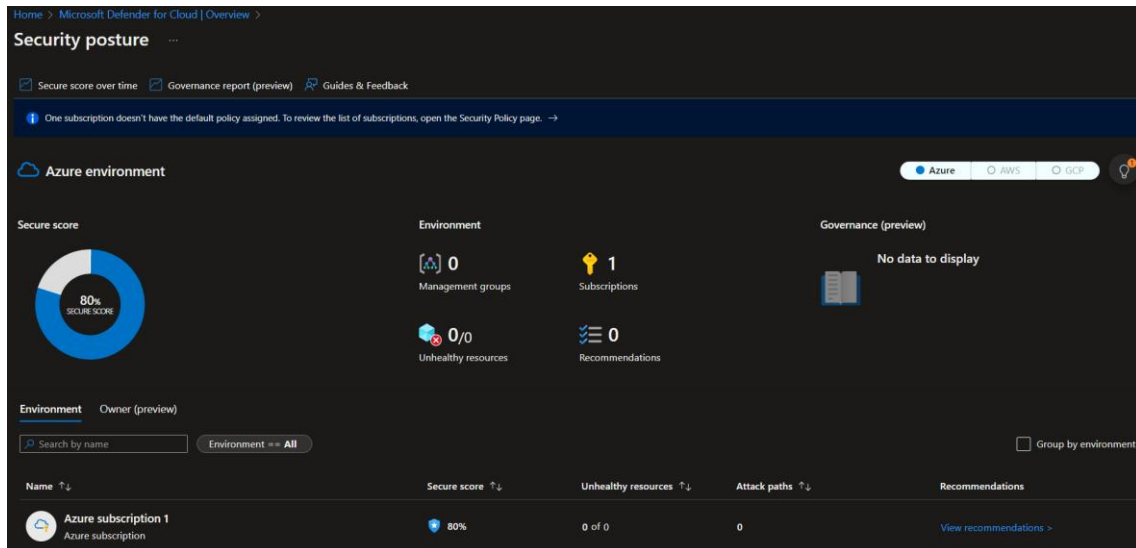


Figure 17. Security posture after configuration changes

#### 5.1.1. Azure Policy Service

The noncompliant policies of System and Communications Protection: SC-7 Boundary Protection Control become partially compliant after executing the Microsoft Defender for

Cloud Service's recommended configuration changes shown in figure 18. The overall compliance achieved 21% which is considered appropriate in scope of the number of selected controls.

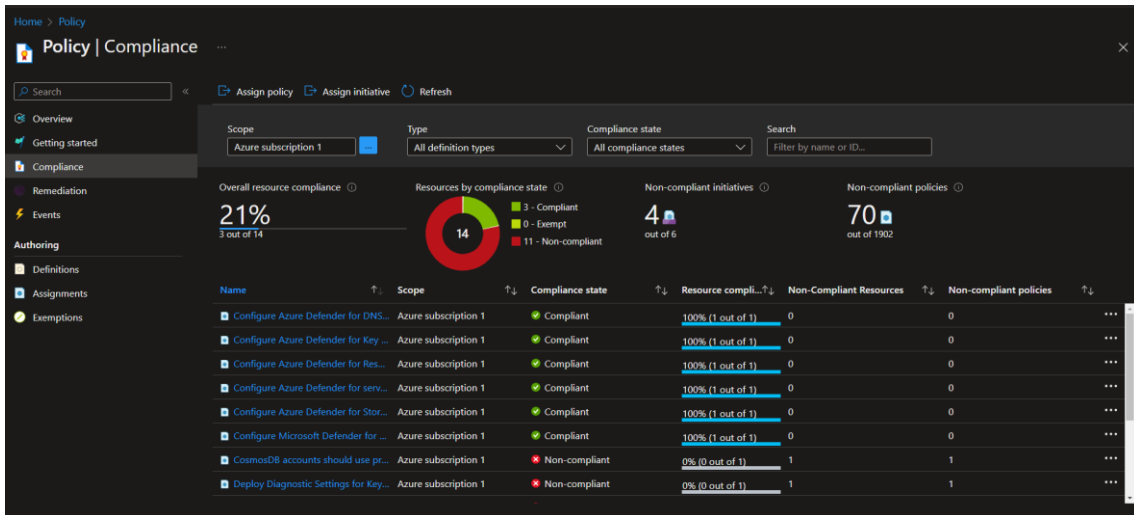


Figure 18. Policy compliance after configuration changes

### 5.1.2. Microsoft Defender for Cloud

As shown in figure 19 "CosmosDB accounts should use private link" policy remained noncompliant after the recommended configuration changes were deployed. The root cause of the noncompliance requires further analysis.

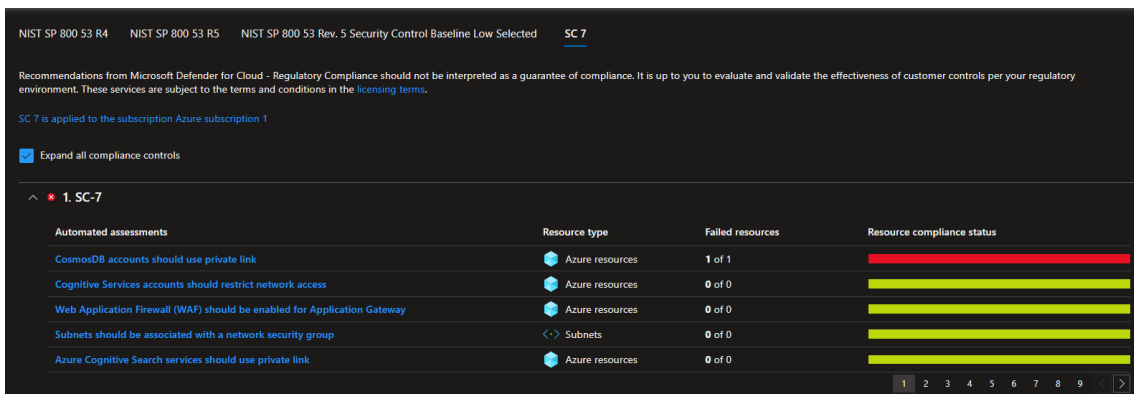


Figure 19. Microsoft Defener for Cloud after configuration changes

### 5.1.3. Microsoft Sentinel Service

As a result of changes made to the other two services of the Microsoft Compliance Ecosystem, the Communications Protection: SC-5 Denial-of-service Protection Control compliance status has been changed from non-applicable

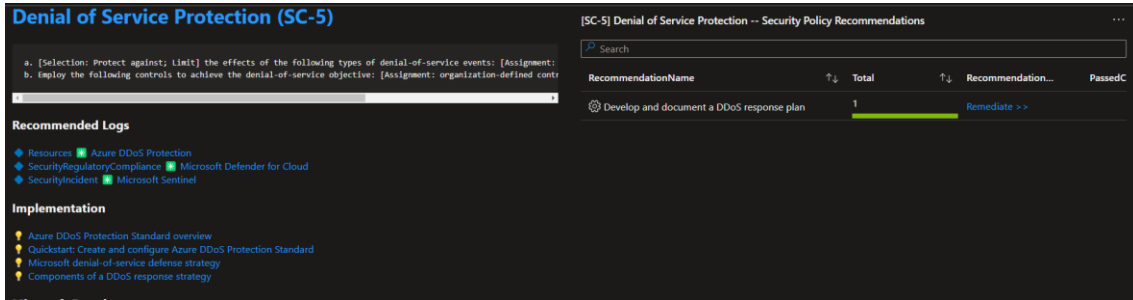


Figure 20. Microsoft Sentinel SC-5 control after configuration changes

In Communications Protection: SC-7 Boundary Protection Control, additional noncompliant policies were identified. The reason for the difference is that the Microsoft Sentinel service also collects information regarding control enhancements, which were not included in the project's scope.

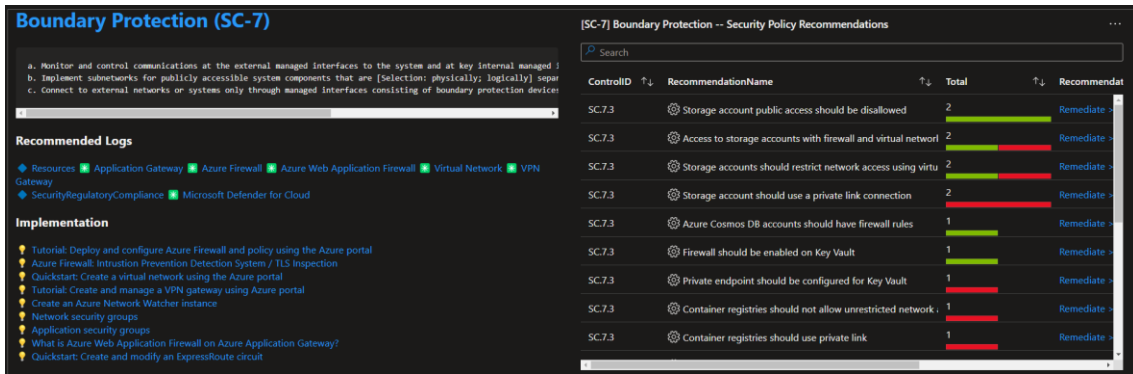


Figure 21. Microsoft Sentinel SC-7 control after configuration changes

## **5.2. Cloudflare Compliance Results**

The protected Domain Name is configured with DNS, TLS, WAF and DDoS protection in order to achieve compliance with the System and Communications Protection: SC-5 Denial-of-service Protection Control and System and Communications Protection: SC-7 Boundary Protection Control. The successful implementation resulted 43 threats which stopped within the last 24 hours.

### **5.2.1. DNS Settings:**

The protected Domain Name has been set up with three DNS records, and DNSSEC has been enabled. Once the DNSSEC-protected zones have been configured, they are cryptographically signed to ensure that the DNS records received are identical to the DNS records published by the domain owner.

The changes in configurations align with System and Communications Protection: SC-7 Boundary Protection Control

## DNS Records

Manage DNS records of your domain. [Documentation](#)

A few more steps are required to complete your setup. [Hide](#)

✓ Add an MX record for your **root domain** so that mail can reach @**jojobworks.com** addresses or [set up restrictive SPF, DKIM, and DMARC records](#) to prevent email spoofing. [New Alert](#)

DNS management for **jojobworks.com**

All changes made in the edit drawer are implemented once saved. [Import and Export](#) [Dashboard Display Settings](#)

Search DNS Records

[Add filter](#)  [Search](#) [Add record](#)

Type ▲	Name	Content	Proxy status	TTL	Actions
A	api	20.0.228.156	Proxied	Auto	<a href="#">Edit ▶</a>
A	*	20.0.228.156	Proxied	Auto	<a href="#">Edit ▶</a>
A	jojobworks.com	20.0.228.156	Proxied	Auto	<a href="#">Edit ▶</a>

Cloudflare Nameservers

To use Cloudflare, ensure your authoritative DNS servers, or nameservers have been changed. These are your assigned Cloudflare nameservers.

Type	Value
NS	diva.ns.cloudflare.com
NS	josh.ns.cloudflare.com

Figure 22. Cloudflare DNS with changed settings

### 5.2.2. SSL/TLS

The SSL/TLS encryption mode has been set to Full (strict) which encrypts end-to-end, but requires a trusted CA or Cloudflare Origin CA certificate on the server. To solve this problem an active and a backup Cloudflare Origin CA certificate were assigned to the platform and the following hardening setting were made:

1. The platform enforces the use of HTTPS by redirecting all requests with scheme "http" to "https". And this change applies to all http requests to the zone.
2. The minimum TLS version has been set to TLS 1.3 which restricts HTTPS connections to visitors who support the selected TLS protocol version or greater.
3. The Author has configured Opportunistic Encryption in order to take advantage of the

improved performance of HTTP/2 by informing browsers that the Author's site is available over an encrypted connection.

After these configuration changes the System and Communications Protection: SC-7 Boundary Protection Control considered compliant in scope of SSL/TLS

## SSL/TLS

Overview [Documentation](#)

The screenshot displays the Cloudflare SSL/TLS configuration interface. At the top, a green checkmark indicates that the SSL/TLS encryption mode is set to 'Full (strict)', with a note that this setting was last changed 2 months ago. Below this, a diagram illustrates the traffic flow: a Browser connects to Cloudflare, which then connects to the Origin Server. The Cloudflare node is highlighted with an orange circle. To the right of the diagram, four radio button options are listed: 'Off (not secure)', 'Flexible', 'Full', and 'Full (strict)'. The 'Full (strict)' option is selected. Below the options, there is a link to 'Learn more about End-to-end encryption with Cloudflare.' and a button to 'Create a Configuration Rule to customize these settings by hostname.' At the bottom right of the main settings area, there are links for 'API' and 'Help'. Below the main settings area, there is a section for 'SSL/TLS Recommender' with a toggle switch that is turned on, and a 'Help' link at the bottom right.

Figure 23. Cloudflare SSL/TLS with changed settings

### 5.2.3. Security Settings

The Author has set the Web Application Firewall configuration to block unwanted traffic communicating with the Domain Name. The following rules are made: deny the requests made by known bots or deny the requests whose threat score equals or is greater than level 6.

Based on the characteristics of the infrastructure, these changes fulfil the Communications Protection: SC-5 Denial-of-service Protection Control in case of Web Application Firewall rules. In the last 24 hours 49 malicious requests were denied by the rules.

# Security - Firewall rules

## WAF (Web Application Firewall)

The Cloudflare WAF provides both automatic protection from vulnerabilities and the flexibility to create custom rules. The order of the rules tabs below represents the sequence of traffic except for tools. [Documentation](#)

[Firewall rules](#)   [Rate limiting rules](#)   [Managed rules](#)   [Tools](#)

[← Back to rules list](#)

### Edit firewall rule

Rule name (required)

SC-5 rule

Give your rule a descriptive name

When incoming requests match...

Field	Operator	Value	
Known Bots	equals	<input checked="" type="checkbox"/>	And X
Or			
Threat Score	greater than or ...	6	And Or X
		e.g. 5	

Expression Preview

[Edit expression](#)

(cf.client.bot) or (cf.threat\_score ge 6)

Then... [About firewall actions](#)

Choose an action (Required)

Block

Figure 24. Cloudflare Security - WAF changed settings

The other configuration change made is setting up DDoS protection. The Author has selected the default ruleset with high sensitivity which complies with the requirements of the SC-5 control.



- ← jobworks.com ▶
- Overview
- Analytics ▼
- DNS ▼
- Email ▼
- SSL/TLS ▼
- Security ▲
- Events
- WAF
- Page Shield
- Bots
- DDoS**
- Settings
- Access
- Speed ▼
- Caching ▼
- ⏪ Collapse sidebar

## Security

[← Back to DDoS](#)

**Configure override** [More About DDoS Protection](#)

### Override configuration

Override name (Required)

SC-5 DDoS Protection

Override scope

Configure when to execute using a range of request parameters.

DDoS L7 ruleset will execute

↳ All incoming requests to jobworks.com

### DDoS L7 ruleset configuration

#### Ruleset configuration

Ruleset action (Required)

Default ▼

Select an action for all rules in the ruleset.  
Default applies each rule's default action.

Ruleset sensitivity (Required)

High ▼

Select a sensitivity for all rules in the ruleset.

Figure 25.. Cloudflare Security - DDoS changed settings

## **6. Summary**

Summarising the findings of the NIST SP 800-53 Revision 5 Standard Compliance at a modelled IT Startup, applicability analysis and implementation of the selected controls were successful within the defined scope and limitations. The Microsoft Azure Platform was an appropriate choice for IaaS platform selection, achieving compliance with the NIST SP 800-53 Revision 5 Standard can be managed with its built-in solutions.

Achieving compliance outside the platform is fulfilled but cannot be automated as inside the IaaS environment, and requires independent configuration for each service, technology, software, hardware, and tool.

### **6.1. Conclusion**

After analysing the implementation and applicability of the selected controls, the Author concludes that this paper could provide guidance about achieving compliance in a pre-defined scope on the Microsoft Azure IaaS platform. However, infrastructures, their elements, selected controls and utilised services in other projects may vary. Which means it is only recommended to do the exact same implementation of controls except if the project in scope is a clone of the introduced startup model, which will not be available to the public.

The process of selecting controls can be achieved in the same way, which could make control selection and implementation in the Microsoft Azure Platform easier for individuals and organisations. For this purpose, the Author shared the control selection Microsoft Excel spreadsheet with the public.

Compliance with NIST SP 800-53 Revision 5 in Microsoft Azure Platform can be achieved in the introduced way independently of the number and type of Azure resources. However, one should take into consideration making the control selection before configuring the Azure Compliance Ecosystem services because otherwise, the assigned policies could contain non-applicable policies with zero assigned Azure resources.

## **6.2. Further works**

As mentioned in Section 5 noncompliant elements will be revised, and a document addressing the remaining applicability analysis and implementation will be written.

The modelled startup infrastructure will be deployed for the public. After achieving full compliance with the NIST SP 800-53 Revision 5 Low Security Baseline, the model will comply with the Moderate Security Baseline, then the High Security Baseline. Furthermore, after achieving these milestones, the model should comply with all applicable controls described in the NIST SP 800-53 Revision 5 standard.

For documenting further applicability analyses and implementation, a separate document will be written and will be stored on the Author's Microsoft OneDrive platform. The platform will be accessible to the public, and One can revise the anonymised documentation, including reports, analyses, implementation guides and policies [24].

## **Acknowledgements**

As the author of this paper, I wish to express my profound gratitude to my supervisors, Kaido Kikkas and Gabor Jeney. Through their supervision of the thesis, I was able to achieve a higher level of quality than I could have achieved on my own. Furthermore, I would like to thank Zoltán Vinda and Imre Balogh, who were part of the team that developed the startup infrastructure model. Through their expertise, insights, and guidance, I was able to improve my thesis and myself during the research process. In addition, I would like to express my gratitude to those friends and family members who supported me during this difficult time.

# Bibliography

- [1] Microsoft, "Microsoft Azure," [Online]. Available: <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-computing/#benefits>. [Accessed 05 01 2023].
- [2] CloudZero, "CloudZero," [Online]. Available: <https://cloudzero.com/blog/cloud-computing-statistics>. [Accessed 05 01 2023].
- [3] eurostat, "eurostat Statistics Explained," [Online]. Available: [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud\\_computing\\_-\\_statistics\\_on\\_the\\_use\\_by\\_enterprises#Enterprises\\_using\\_cloud\\_computing](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises#Enterprises_using_cloud_computing). [Accessed 05 01 2023].
- [4] NIST, "Control Baselines for Information Systems and Organizations," [Online]. Available: <https://csrc.nist.gov/publications/detail/sp/800-53b/final>.
- [5] National Institute of Standards and Technology, Control Baselines for Information Systems and Organizations, NIST, 2020.
- [6] National Institute of Standards and Technology, NIST Special Publication 800-53A Revision 5, NIST, 2020.
- [7] National Institute of Standards and Technology, NIST Special Publication 800-53B, NIST, 2020.
- [8] NIST, "NIST Special Publication 800-53 Revision 5," in *Security and Privacy Controls for Information Systems and Organizations*, NIST.
- [9] Microsoft, "Azure documentation," [Online]. Available: <https://learn.microsoft.com/en-us/azure/?product=popular>. [Accessed 05 01 2023].
- [10] AWS, "amazon web servies," [Online]. Available: <https://aws.amazon.com/compliance/nist/>.
- [11] Google, "Google Cloud," [Online]. Available: <https://cloud.google.com/security/compliance/nist800-53>.
- [12] Microsoft, "Microsoft Learn," [Online]. Available: <https://learn.microsoft.com/en-us/azure/governance/policy/samples/nist-sp-800-53-r5>.

- [13] Microsoft, "Azure Solutions," [Online]. Available: <https://azure.microsoft.com/en-us/solutions/>. [Accessed 05 01 2023].
- [14] Benedek, "OneDrive - Selectedcontrols.xlsx," 05 01 2023. [Online]. Available: [https://1drv.ms/x/s!Apcn90FwIR0ib73gq\\_QLkLqyl\\_A?e=miBcEF](https://1drv.ms/x/s!Apcn90FwIR0ib73gq_QLkLqyl_A?e=miBcEF). [Accessed 05 01 2023].
- [15] Microsoft, "Details of the NIST SP 800-53 Rev. 5 Regulatory Compliance built-in initiative," [Online]. Available: <https://learn.microsoft.com/en-us/azure/governance/policy/samples/nist-sp-800-53-r5>.
- [16] M. Azure, "Azure compliance documentation," [Online]. Available: <https://learn.microsoft.com/en-us/azure/compliance/>. [Accessed 05 01 2023].
- [17] M. Azure, "Azure Policy documentation," [Online]. Available: <https://learn.microsoft.com/en-us/azure/governance/policy/>. [Accessed 05 01 2023].
- [18] Microsoft, "Microsoft Defender for Cloud," [Online]. Available: <https://www.microsoft.com/en-us/security/business/cloud-security/microsoft-defender-cloud>. [Accessed 05 01 2023].
- [19] Microsoft, "Microsoft Sentinel documentation," [Online]. Available: <https://learn.microsoft.com/en-us/azure/sentinel/>. [Accessed 05 01 2023].
- [20] Cloudflare, "Cloudflare Docs," [Online]. Available: <https://developers.cloudflare.com/>. [Accessed 05 01 2023].
- [21] Cloudflare, "Manage DNS records," [Online]. Available: <https://developers.cloudflare.com/dns/manage-dns-records/how-to/create-dns-records>. [Accessed 05 01 2023].
- [22] Cloudflare, "Get started with SSL/TLS," [Online]. Available: <https://developers.cloudflare.com/ssl/get-started>.
- [23] Cloudflare, "<https://www.cloudflare.com/learning/dns/dns-security/>," [Online]. Available: <https://www.cloudflare.com/learning/dns/dns-security/>. [Accessed 05 01 2023].
- [24] B. Matveev, "OneDrive - Further Works," 05 01 2023. [Online]. Available: <https://1drv.ms/u/s!Apcn90FwIR0ibpmS-FVmZl1tJLY?e=6Jpsxr>. [Accessed 05 01 2023].
- [25] M. Tierney, "netwrix," [Online]. Available: <https://blog.netwrix.com/2021/03/03/nist-800-53/>.

- [26] O. DataGuidance, "<https://www.dataguidance.com/opinion/usa-nist-sp-800-53-rev-5>," [Online].
- [27] eurostat, [Online]. Available: [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud\\_computing\\_-\\_statistics\\_on\\_the\\_use\\_by\\_enterprises#Enterprises\\_using\\_cloud\\_computing](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises#Enterprises_using_cloud_computing).
- [28] Microsoft, "Microsoft Azure," [Online]. Available: <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-computing/#benefits>.
- [29] NIST, "Information Technology Laboratory - COMPUTER SECURITY RESOURCE CENTER," [Online]. Available: [https://csrc.nist.gov/glossary/term/Blue\\_Team](https://csrc.nist.gov/glossary/term/Blue_Team).
- [30] NIST, "Control Baselines for Information Systems and Organizations," [Online]. Available: <https://csrc.nist.gov/publications/detail/sp/800-53b/final>.

# Appendices

## Appendix 1 – Non-Exclusive License

I Benedek Matveev

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis "The NIST SP 800-53 Revision 5 Standard Compliance at IT Startups: an Applicability Analysis and Implementation", supervised by Kaido Kikkas and Gabor Jeney
  - 1.1 to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
  - 1.2 be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the Author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

Date: 01.05.2023



## Appendix 2 – Supporting Tables:

### 1. NIST SP 800-53 Revision 5 Control Families Table:

ID	Family Name	Examples of Controls
AC	Access Control	Account management and monitoring; least privilege; separation of duties
AT	Awareness and Training	User training on security threats; technical training for privileged users
AU	Audit and Accountability	Content of audit records; analysis and reporting; record retention
CA	Assessment, Authorisation, and Monitoring	Connections to public networks and external systems; penetration testing
CM	Configuration Management	Authorised software policies, configuration change control
CP	Contingency Planning	Alternate processing and storage sites; business continuity strategies; testing
IA	Identification and Authentication	Authentication policies for users, devices and services; credential management
IP	Individual Participation	Consent and privacy authorisation
IR	Incident Response	Incident response training, monitoring and reporting
MA	Maintenance	The system, personnel and tool maintenance
MP	Media Protection	Access, storage, transport, sanitisation, and use of media
PA	Privacy Authorisation	Collection, use and sharing of personally identifiable information (PII)
PE	Physical and Environment Protection	Physical access; emergency power; fire protection; temperature control
PL	Planning	Social media and networking restrictions; defence-in-depth security architecture
PM	Program Management	Risk management strategy; <u>insider threat</u> program; enterprise architecture
PS	Personnel Security	Personnel screening, termination and transfer; external personnel; sanctions
RA	Risk Assessment	Risk assessment; vulnerability scanning; privacy impact assessment

SA	System and Services Acquisition	System development lifecycle; acquisition process; supply chain risk management
SC	System and Communications Protection	Application partitioning; boundary protection; cryptographic key management
SI	System and Information Integrity	Flaw remediation; system monitoring and alerting

Table 2. List of control families [25]

## 2. Table of Selected Controls:

Control (or Control Enhancement) Name	Control Identifier	Control Family	Security Control Baseline - Low
Account Management	AC-2	Access Control	x
Access Enforcement	AC-3	Access Control	x
Unsuccessful Logon Attempts	AC-7	Access Control	x
Permitted Actions Without Identification or Authentication	AC-14	Access Control	x
Remote Access	AC-17	Access Control	x
Use of External Systems	AC-20	Access Control	x
Publicly Accessible Content	AC-22	Access Control	x
Event Logging	AU-2	Audit and Accountability	x
Content of Audit Records	AU-3	Audit and Accountability	x
Audit Log Storage Capacity	AU-4	Audit and Accountability	x
Response to Audit Logging Process Failures	AU-5	Audit and Accountability	x
Audit Record Review, Analysis, and Reporting	AU-6	Audit and Accountability	x
Time Stamps	AU-8	Audit and Accountability	x
Protection of Audit Information	AU-9	Audit and Accountability	x
Audit Record Retention	AU-11	Audit and Accountability	x

Audit Record Generation	AU-12	Audit and Accountability	x
Information Exchange	CA-3	Assessment, Authorisation, and Monitoring	x
Continuous Monitoring	CA-7	Assessment, Authorisation, and Monitoring	x
Internal System Connections	CA-9	Assessment, Authorisation, and Monitoring	x
Baseline Configuration	CM-2	Configuration Management	x
Impact Analyses	CM-4	Configuration Management	x
Access Restrictions for Change	CM-5	Configuration Management	x
Least Functionality	CM-7	Configuration Management	x
System Backup	CP-9	Contingency Planning	x
System Recovery and Reconstitution	CP-10	Contingency Planning	x
Identification and Authentication (organisational Users)	IA-2	Identification and Authentication	x
Identifier Management	IA-4	Identification and Authentication	
Authenticator Management	IA-5	Identification and Authentication	x
Cryptographic Module Authentication	IA-7	Identification and Authentication	x
Identification and Authentication (non-organisational Users)	IA-8	Identification and Authentication	x
Incident Handling	IR-4	Incident Response	x
Incident Monitoring	IR-5	Incident Response	x
Media Access	MP-2	Media Protection	x
Media Sanitization	MP-6	Media Protection	x
Rules of Behavior	PL-4	Planning	x
Security Categorisation	RA-2	Risk Assessment	x
Risk Assessment	RA-3	Risk Assessment	x
Vulnerability Monitoring and	RA-5	Risk Assessment	x

Scanning			
Denial-of-service Protection	SC-5	System and Communications Protection	x
Boundary Protection	SC-7	System and Communications Protection	x
Cryptographic Key Establishment and Management	SC-12	System and Communications Protection	x
Cryptographic Protection	SC-13	System and Communications Protection	x
Collaborative Computing Devices and Applications	SC-15	System and Communications Protection	x
Secure Name/address Resolution Service (authoritative Source)	SC-20	System and Communications Protection	x
Secure Name/address Resolution Service (recursive or Caching Resolver)	SC-21	System and Communications Protection	x
Architecture and Provisioning for Name/address Resolution Service	SC-22	System and Communications Protection	x
Process Isolation	SC-39	System and Communications Protection	x
Flaw Remediation	SI-2	System and Information Integrity	x
Malicious Code Protection	SI-3	System and Information Integrity	x
System Monitoring	SI-4	System and Information Integrity	x
Security Alerts, Advisories, and Directives	SI-5	System and Information Integrity	x

Table 3. List of selected controls