

Oyebamiji Oluwafemi Oyedokun
Department of Computer Science (Applied Computing)
University of Wale Trinity Saint David
Quay Place, Louisa House, Birmingham, B1 2RA.
2409692@student.uwtsd.ac.uk.

ABSTRACT

This paper looks at how digital governance is changing by combining important ideas from risk management, ethics, compliance, cybersecurity, and legal frameworks. Ethical principles make sure that systems are fair, open, accountable, and protect human rights.

The paper gives Zero Trust Architecture a critical review. Zero Trust Architecture is a new security model that uses continuous proof, least privilege access, and the assumption of breach. Zero Trust provides better security for cloud based and distributed environments compared to standard perimeter-based models. However, it is harder to set up because of issues with identity management, policy complexity, and organisational readiness.

INTRODUCTION

Modern Organization work in a digital world that is changing quickly. This world is made up of interconnected systems, cyber threats, and regulatory pressures that demand better governance. Traditional security and compliance models aren't enough anymore because companies must deal with AI-related risks, observe moral standards, and follow many rules that overlap, like

GDPR, DORA, and NIS2. At the same time, cybersecurity paradigms like Zero Trust question assumptions that are built on perimeters and call for constant verification and controls that focus on identities.

Protecting users, devices, and data that are spread out across hybrid settings is an important part of modern cybersecurity. Companies need to make sure that remote access is safe, that data is well managed, and that identity-centric rules are used.

The report focus on how modern Organization can improve their security by using Zero Trust, keeping hybrid workforces safe, keeping an eye on AI systems, and keeping up with changing rules to protect themselves from cyber threats and respond to them.

1.1 EXPLANATION DATA SECURITY AND COMPLIANCE

Data security can be defined as set of procedures, methods, and guidelines that safeguard data at every stage of its existence, including creation, storage, transfer, and destruction [3].

Compliance can be defined as ability of an organisation to handle data in accordance with legal, regulatory, and industry specific regulations is referred to as compliance [4]. These regulations control are how data and

information is protected, how breaches must be reported, how data and information is stored, how long did data and information are retained and how data and information is collected [4].



Figure 1 image show the understanding Of data security and compliance

1.2 SECURING THE HYBRID WORKFORCE:

Securing the hybrid workforce means that the collection of technology, governance procedures, and security tactics that safeguard company data and systems while workers are employed both on the site and remotely. Organisations must safeguard users, devices, and data wherever they are instead of depending on office-based firewalls or VPNs since hybrid work dissolves the traditional network perimeter [3].

1.2.1 Zero Trust Network Access (ZTNA)

Zero Trust Network Access is a modern security technique that give users identity based, secure access to applications instead of granting them general network access. It applies the Zero Trust principle of “never trust,

always verify” to remote and hybrid access [1].

No matter who the user is, where they are, or what device they are using, ZTNA makes sure that every access request is constantly checked before being approved.

Figure 2 image show ZTNA quotes

The core principle of Zero Trust Network Access (ZTNA) Architecture.

Zero Trust begins with the principle of never trusting and always verifying, meaning every access request must be validated regardless of whether it originates inside or outside the network. It also requires granting only the least privilege necessary so that any breach has a minimal blast radius [1].

The model assumes that attackers may already be present within the environment, which drives the need for micro-segmentation and continuous monitoring. Access decisions rely on conditional access and continuous authentication, incorporating identity assurance, device health, behavioural analytics, and contextual risk [2].

Micro-segmentation further restricts lateral movement by dividing network resources into tightly controlled segments. Finally, Zero Trust depends on distributed Points of Policy Enforcement that apply security rules in real time across the environment [2].

1.2.2 SASE (Secure Access Service Edges)

SASE is a cloud delivered architecture that integrates security and networking into a single, Unified service. These are SD-WAN (Networking), access to Zero Trust Networks (ZTNA), CASB, or Cloud Access Security Broker, SWG, or Secure Web Gateway and Firewall as a Service (FWaaS) [6].

How SASE Protect Data Outside of the Company Boundaries

Secure Access Service Edge (SASE) improves the safety of an organization by using Zero Trust principles, which mean that no person or device is automatically trusted. Access decisions are based on identity, context, and device posture. One time authentication has been replaced by continuous verification, which is an important feature for hybrid workers who join from places that aren't always stable [5].

Since SASE is provided through the cloud, it uses the same security controls everywhere. This gets rid of the problems that come with unmanaged networks and regular VPNs.

Inline threat protection is also offered by SASE. It checks all traffic for malware, phishing attempts, malicious URLs, and risky cloud application behaviour in real time. This kind of proactive filtering stops threats before they can harm users or company data [5].

When combined with a Cloud Access Security Broker (CASB), SASE improves cloud and SaaS security by keeping an eye on cloud usage, blocking shadow IT, enforcing data-sharing policies, and stopping data exfiltration. This is especially important for hybrid teams that use Teams, Slack, OneDrive, and Google Drive a lot [5].

SASE cuts off broad VPN access, limits permissions to specific apps, stops unsafe browsing sessions, and separates people and devices to make them harder to attack. This division stops movement from side to side, which is a big risk in remote access breaches. SASE also makes it easier to predict, find, and respond to threats. AI/ML analytics find odd logins, dangerous device behaviour, strange cloud activity, and possible insider threats, which lets you reduce risk before it happens. SASE can find strange things like impossible travel or a lot of files being downloaded by constantly watching network traffic, cloud API calls, user actions, and data transfers. Response times are cut from hours to seconds by automated actions like stopping malicious sessions, requiring step-up authentication, quarantining devices, and revoke keys [7].

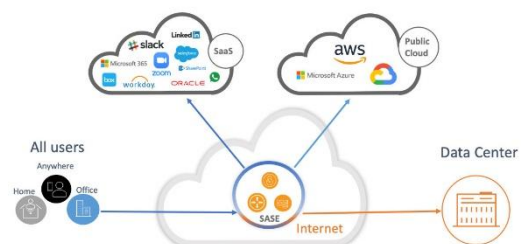


Figure 3 image show how SASE Operate

1.2.3 DLP (Data Loss Prevention)

Data Loss Prevention (DLP) refers to technologies and regulations that identify, track, and stop sensitive data from being moved, shared, or exposed without authorisation [6].

DLP protect utilised data (on endpoints), motion of data (across networks) and data at rest (in databases or cloud storage) [6].

It ensures the private information; including financial records, intellectual property, personal information, and secret papers or intentionally disclosed [6].

How DLP Protects Data Beyond the Corporate Perimeter

Pattern matching, machine learning, contextual analysis, and sensitivity tags like "Internal Only" or "Confidential" are some of the ways that Data Loss Prevention (DLP) systems sort and identify information. This lets the system figure out which info needs to be kept safe [7].

Once classification is done, DLP applies security policies. For example, it stops uploads to personal cloud storage, stops emails from going to people who aren't supposed to get them, stops people from copying, printing, or pasting sensitive files, stops people from using USB drives, and automatically encrypts protected data. These rules are valid both at work and away from work. DLP also keeps an eye on file transfers, email attachments, activity in the cloud, endpoint behaviour, and data moves

that don't make sense. It finds big downloads, suspicious uploads, unauthorised sharing, and possible insider exfiltration, so threats can be found quickly [8].

Today's DLP systems can automatically stop dangerous actions, put files in a safe place, deny access, secure private documents, notify security teams, and give users real-time warnings. This automation cuts down on damage and speeds up the reaction time to an incident [7].

1.3 GOVERNANCE OF AI AND MACHINE LEARNING SYSTEMS:

To make decisions, automate processes, and gain a competitive edge,

1.3.0 Managing Risk

Managing risk systematic process of identifying, evaluating, controlling, and monitoring possible threats that can have a negativity impact on an organization's operations, data, systems, or stakeholders [9].

1.3.1 Ethics

In the AI and machine learning governance, ethics referred as the ideas, beliefs, and standards that dictate how AI systems should be designed, developed, deployed and monitored to make sure they don't damage people and continue to meet society expectation. Ethics is about doing the right thing, not only what is technically possible or mandated by law [9].

Essential elements of ethics

Fairness is the avoidance of discriminatory results, transparency: recording the reasoning behind decisions and the operation of models, assigning accountability for exemplary behaviour is known as accountability and human oversight: making sure that people continue to make important judgements are essential elements of ethics [9].

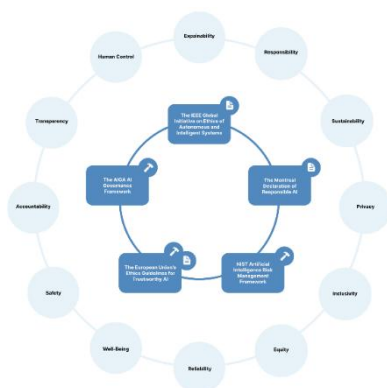


Figure 4 image show governance of AI

1.3.1 compliance for AI data and models.

Compliance for AI data and models referred to ensuring that AI systems, their data, and their outputs abide by all applicable laws, rules, standards, and internal policies.

For example: "What is the right thing to do?" is an ethical question. "What must we do to meet legal and regulatory obligations?" is the question compliance poses.

1.4 THE ZERO TRUST ARCHITECTURE:

1.4.1 Zero Trust Architecture

Zero Trust Architecture is a security paradigm build on the principle

"never trust, always verify" ZTA sees every person, device, task, and data flow as potentially hostile until they are continually authenticated, authorised, and verified, rather than presuming that everything inside the network perimeter is trustworthy [14].

Zero Trust Architecture is shown in the below diagram as a system where users and devices must register with an identity provider before a central policy engine checks the risk and lets them in. Protected resources can only be accessed after being verified, and they are constantly being watched to find strange behaviour and keep security high.

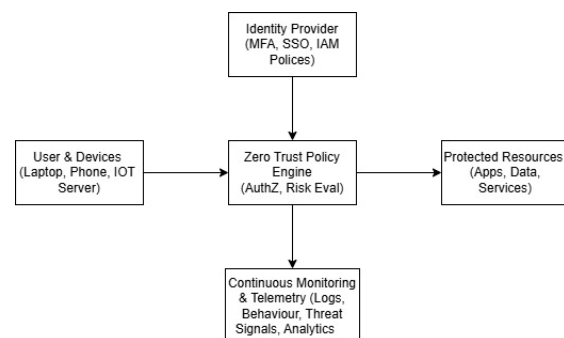


Figure 5 image show the conceptual diagram for ZTA

1.4.2 Critical Analysis for principle of Zero Trust Architecture.

Zero Trust Architecture is based on continuous, context aware verification. Instead of giving access forever, it is constantly reevaluated based on identity, device posture, location, activity, and risk signals. Granular tools like micro segmentation and just in time rights make sure that users and services only get the access

they need. This is called least privilege access [15].

ZTA stops people from moving laterally and lessens the damage of possible breaches by thinking that attackers might already be in the environment. At its heart, this model is strong identity and device security, which is backed up by multifactor authentication, regular compliance checks, and ongoing posture assessments. But how well it works rests a lot on how well the identity systems, policy design, and monitoring tools are working [16].

This means that managing identities and telemetry is more complicated than managing network edges [16].

1.4.3 Implementation challenges

Organisation with old or mixed infrastructures find it hard to implement Zero Trust Architecture because their older systems often can't handle micro-segmentation, strong identity controls, or fine-grained policies. This makes upgrading expensive and time-consuming [15].

The model also needs complicated policy design that considers the situation. Rules that aren't structured well can lead to operational friction, access issues, and policy sprawl. Rich telemetry, like identity logs, device posture, network flows, and application behaviour, is needed for Zero Trust to work, but many Organisations don't have the analytics maturity and integration tools to make good use of this data [16].

There is also cultural pushback because Zero Trust changes long-held beliefs about trust and access, which users and IT teams often find annoying. Also, putting ZTA into action usually requires a lot of different security tools, which makes integration expensive and hard, and the fact that different vendors make it harder to see what the real design needs are [16].

1.4.4 Efficacy compared to traditional models.

Table 1 show Efficacy compared to traditional models.

Aspect	Traditio nal perimete r	Zero Trust Architecture
Trust Model	Verify at the edge and trust inside.	Always verify and never trust
Boundary	Network Perimeter (firewalls, VPN).	Data, device, identity and workload.
Assumpti on	Inside equal to save and outside is equal to hostile.	Breach is inevitable/ongoing.
Access Control	Network centric and coarse grained.	Policy centric and fine grained.
Fit for cloud /remote work	Poor	Strong.

1.5 Compliance in a Fragmented World:

1.5.1 Compliance in a Fragmented World

Compliance in a Fragmented World refers to the challenges that organisations confront while attempting to satisfy numerous, overlapping, and occasionally contradicting regulatory obligations across several countries, sectors, and technical domains [18].

1.5.2 Navigating GDPR, alongside new regulations like DORA (Digital Operational Resilience Act)

The General Data Protection Regulation (GDPR) is the main piece of legislation used by the European Union to protect personal information and people's right to privacy. It came into force on 25 May 2018 and is widely regarded as the most comprehensive data protection law in the world [19].

GDPR: Data Protection and Individual Right:

The General Data Protection Regulation (GDPR) is the EU's main law for protecting personal data. It includes rules on handling that is lawful, fair, and clear, as well as rules on data minimisation, purpose limitation, accountability, documentation, and strong security measures. It also protects important personal rights, like the ability to view, delete, and move data. Organisations must follow strong data-handling procedures to comply with GDPR [18].

These include only taking information that is needed, keeping it safe, keeping clear records of

processing activities, being open with data subjects, and letting people use their rights. As part of compliance, the right technical and organisational controls must be put in place, assessments must be done regularly, and responsibility must be shown throughout the data lifecycle [18].

DORA: Digital Operational Resilience ACT:

The Digital Operational Resilience Act (DORA) is an EU law that makes sure financial institutions, and their ICT service providers can handle, react to, and recover from problems caused by technology. It sets rules for managing ICT risks, reporting incidents, testing operating resilience, having a third party oversee risk, and sharing information.

To follow DORA, Organisation need to have strong ICT governance, keep detailed incident handling processes, test their digital resilience on a regular basis, and keep a close eye on the risks that come from using technology from outside the Organisation. They also need to make sure there is clear paperwork, constant monitoring of important systems, and the ability to show regulators that they are following the rules.

1.5.3 NIS2 for critical infrastructure

The European Union's new cybersecurity regulation, NIS2, replaces the NIS regulation from 2016 and makes protections stronger for key and crucial areas. It sets tougher rules for finding and reporting incidents, keeping the supply chain safe, holding executives accountable, managing

cybersecurity risks, keeping the Organization running, and planning for how to handle a crisis. To respect NIS2, organisations must implement robust security controls, maintain clear oversight of third-party risks, ensure timely reporting of significant incidents, and establish strong continuity and crisis-management procedures [19].

1.5.4 GDPR, DORA, NIS2 focus, sector and core objective.

Table 2 shows GDPR, DORA, NIS2 focus, sector and core objective.

Regulation	Focus	Sector	Core Objective
GDPR	Data protection and privacy	All sector	Protect personal data
DORA	Operational resilience	Financial Sector	Ensure continuity of financial service
NIS2	Cybersecurity and critical infrastructure	Essential and important entities	Strengthen EU wide cyber resilience.

1.5.5 Why fragmentation matter

Fragmented regulations make it more expensive for Organization to follow the rules because they must deal with multiple frameworks that overlap and have different meanings and requirements. It makes reporting less

clear, puts more stress on supply lines, and requires GDPR, DORA, and NIS2 to all be governed by the same rules [20].

Complexity can be a problem, but mature companies with good risk and cybersecurity practices can use it to their benefit [20].

1.6 Conclusion

In conclusion, through the integration of risk, ethics, compliance, and contemporary cybersecurity across Organisation, a unified governance strategy enhances resilience. Zero Trust, strong data governance, and hybrid-work security together ensure resilient, compliant protection in modern organizations.

1.7 REFERENCES

- [1] National Institute of Standards and Technology (NIST), *Zero Trust Architecture*, NIST Special Publication 800-207, 2021.
- [2] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," *NIST SP 800-207*, pp. 1-59, Aug. 2021.
- [3] Gartner, "The Future of Network Security Is in the Cloud," *Gartner Research*, 2021.
- [4] European Union, *General Data Protection Regulation (GDPR)*, Regulation (EU) 2016/679, 2022.
- [5] N. Mavroeidis and J. Bromander, "Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence," *Journal of*

Cyber Security Technology, vol. 3, no. 3, pp. 1-29, 2021.

[6] Gartner, “Market Guide for Data Loss Prevention,” Gartner Research, Stamford, CT, USA, 2023.

[7] A. Singh and K. Chatterjee, “Cloud Security Issues and Challenges: A Survey,” *Journal of Network and Computer Applications*, vol. 79, pp. 88–115, Feb. 2022.

[8] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture,” National Institute of Standards and Technology (NIST), Special Publication 800-207, Aug. 2021.

[9] A. Author, *Managing Risk, Ethics, and Compliance for AI Data and Models. USA, 2021.

[10] National Institute of Standards and Technology, “Artificial Intelligence Risk Management Framework (AI RMF 1.0),” NIST, Gaithersburg, MD, USA, 2023.

[11] European Commission, “Ethics Guidelines for Trustworthy AI,” High-Level Expert Group on Artificial Intelligence, Brussels, Belgium, 2021.

[12] S. Mittelstadt, P. Allo, M. Taddeo, S. Wachter, and L. Floridi, “The ethics of algorithms: Mapping the debate,” *Big Data & Society*, vol. 3, no. 2, pp. 1–21, 2022.

[13] L. Floridi and J. Cows, “A unified framework of five principles for AI in society,” *Harvard Data Science Review*, vol. 1, no. 1, 2021.

[14] IBM Security, “Zero Trust Security: A Strategy for Modern Threats,” IBM Corporation, Armonk, NY, USA, 2022.

[15] National Institute of Standards and Technology, “Zero Trust Architecture,” NIST Special Publication 800-207, Gaithersburg, MD, USA, 2021.

[16] Gartner, “Zero Trust Is an Essential Strategy for Modern Cybersecurity,” Gartner Research, Stamford, CT, USA, 2023.

[17] European Union, “Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS2 Directive),” Official Journal of the European Union, 2022.

[18] ENISA, “Cybersecurity Requirements for Critical Infrastructure under NIS2,” ENISA, 2023.

[19] KPMG, “Navigating NIS2: Compliance Obligations for Critical and Essential Entities,” KPMG Cyber Security Report, 2023.

[20] European Commission, “Questions and Answers: NIS2 Directive,” European Commission, Brussels, Belgium, 2023.



MediTrust Analytics Zero Trust Security Programme for EU Operations

By

OYEBAMIJI OLUWAFEMI OYEDOKUN

2409692@student.uwtsd.ac.uk

University of Wales Trinity Saint David

Quay Place Campus, 92-93 Edward St, Birmingham B1 2RA

Table of content

Title Page.....	10
Table of Contents	11
Abstract	12
Introduction	13
1.0 Organisation Structure.....	14
2.0 Policies & Procedures.....	15
2.1 Develop policies for AI Usage.....	16
2.2 Secure SaaS Configuration.....	16
2.3 BYOD for a hybrid workforce.....	17
2.3.1 Technical support for BYOD	17
3.0 Compliance	17
3.1 DORA's operational resilience requirements	18
3.2 NIS2 reporting obligations	19
4.0 Governance & Strategy	20
4.1 Governance Model for MediTrust Based on NIST CSF 2.0	20
4.2 Linking Security Strategy to Business Goals	21
5.0 Risk Management	22
5.1 High-level risk assessment focusing on software supply chain risks	22
5.2 Cloud Misconfigurations	24
6.0 Contingency Planning	25
6.1 Disaster Recovery Plan for Ransomware Attack	25
7.0 Protection Mechanisms.....	27
7.1 Modern Security Controls	27
References	28

Abstract

MediTrust Analytics is entering the EU healthcare industry and must enhance its cybersecurity measures to comply with GDPR, DORA, and NIS2 requirements. The organization has adopted a cohesive Zero Trust security framework, overseen by the CISO and bolstered by five specialised divisions.

Governance, Risk, and Compliance guarantee regulatory conformity, whereas Zero Trust and IAM Engineering safeguard identity, access, and infrastructure.

Cloud Security Architecture safeguards multi-cloud setups and ensures compliance with EU data residency regulations. Digital resilience and security operations provide ongoing monitoring and incident response.

The AI, Data and Security Division protects model integrity and sensitive clinical datasets, ensuring reliability and operational resilience.

Introduction

MediTrust Analytics is moving into the EU healthcare industry, and to meet GDPR, DORA, and NIS2 standards, it needs to improve its security. The organization has set up a single security model that is overseen by the CISO and backed by five specialised divisions to make this happen.

Governance, Risk, and Compliance makes sure that rules are followed, while Zero Trust and IAM Engineering protect identity, access, and infrastructure. Cloud Security Architecture keeps multi-cloud environments safe and EU data safe.

Digital Resilience and Security Operations keep an eye on things all the time and respond to incidents. The AI, Data, and Security Division protects model integrity and sensitive clinical datasets as part of a full Zero Trust approach.

This report focuses on how MediTrust can improve its security and resilience by switching to Zero Trust, following EU rules, protecting its cloud and AI systems, and using up to date controls to stop, identify, and recover from attacks.

1.0 Organisation Structure

An organization structure is a means to set up cybersecurity so that the way the organization is set up becomes a way to regulate it. This approach doesn't see security as a set of technological tools. Instead, it makes security part of roles, reporting lines, responsibilities, and governance bodies. It makes sure that people, teams, and the way decisions are made are all in line with the organization's risk profile, regulatory requirements, and strategic goals [1].

The diagram below shows how MediTrust Analytics Ltd EU Information Security Unit is set up, with a Chief Information Security Officer (CISO) reporting to the Board to make sure everyone is accountable and follows the rules. It has four main divisions: Governance, Risk & Compliance (GRC); Zero Trust & Security Engineering; Digital Resilience & Security Operations; and AI & Data Security. The GRC team is in charge of following the rules and managing third-party risk. Security Engineering uses Zero Trust, which includes protecting identities and the cloud. A Cloud Security Architect leads this work. The SOC makes sure that monitoring and responding to incidents happen [3].

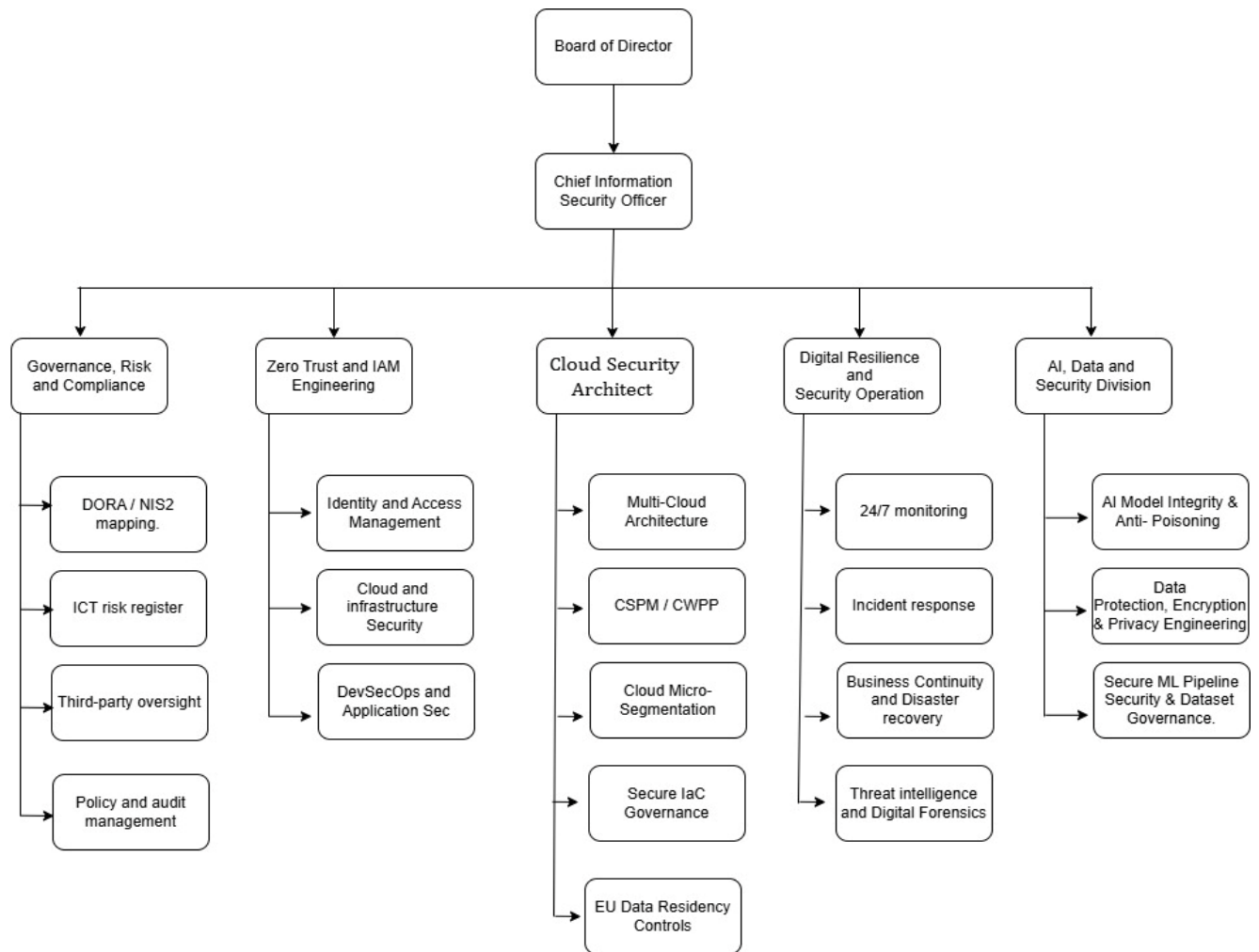


Figure 1 diagram shows the organisation structure design.

2.0 Policies & Procedures

Policies and procedures are a governance driven method in which an organization secures itself by setting explicit rules, writing down expectations, and creating repeatable processes that tell staff, systems, and data how to act. This model doesn't just rely on technology; it also includes written policies, standards, and procedures as rules that people must follow. These rules shape behaviour, make things less confusing, and make sure that people follow the law [2].

2.1 Develop policies for AI Usage

MediTrust's AI policy makes ensuring that AI is created and used in a safe, ethical, and legal way that meets all rules and regulations. It applies to everyone who works with AI systems or data, including employees, developers, analysts, and third parties. MediTrust's can only utilise AI tools for business goals that have been permitted. The public generative AI platforms to handle private or sensitive information should not be used. The patient data, proprietary models, or internal research materials to external services should not be upload without getting permission and a security check. When possible, AI training data must be anonymised or tokenised. Access to datasets is limited depending on role and need [3].

2.2 Secure SaaS Configuration

Software as a Service (SaaS) configuration refer to the establishment and administration of security measures, access restrictions, and operational parameters for a Software as a Service (SaaS) application to guarantee its secure functioning in alignment with organisational standards [4].

The Secure SaaS Configuration Policy in MediTrust rules should set to make sure that all Software as a Service (SaaS) platform utilised by the company are set up and run in a safe way. The policy should cover employees, administrators, developers, and third-party partners who use or operate SaaS apps for business administration, data analysis, collaboration, or clinical operations. It is meant to keep sensitive healthcare data safe, keep the system running smoothly, and make sure that the EU's Digital Operational Resilience Act and Directive on Security of Network and Information Systems are followed [4].

2.3 BYOD for a hybrid workforce

BYOD for a hybrid workforce refers to the Bring Your Own Device policy, which permits employees to use their personal devices (such laptops, Telephones and tablets) to access business systems and execute professional activities while operating both remotely and in the office [5].

2.3.1 Technical support for BYOD

BYOD devices must go through strict identity verification, which includes multifactor authentication, limited access, and device posture checks. The Cloud Security Architect makes sure that micro-segmentation is followed so that personal devices can only access approved SaaS apps or VDI environments. This stops lateral movement into private clinical data for EU residents. The AI, Data, and Security Division makes sure that no patient data is kept locally by directing access through encrypted containers or browser-isolated workspaces. These are backed up by DLP controls that stop people from taking screenshots, copying, or syncing without permission. Continuous tracking finds devices that have been hacked or acting in a strange way, and Governance, Risk, and Compliance makes sure that all GDPR, DORA, and NIS2 rules are followed.

3.0 Compliance

Compliance refers to following laws, rules, standards, and organisational policies pertinent to a company's activities. In cybersecurity and information security, compliance ensures that an organization secure data, effectively manages risks, and operates according to required legal and regulatory frameworks [7].

3.1 DORA's operational resilience requirements

The operational resilience mandates of the Digital Operational Resilience Act (DORA) are rules that require organisations within the financial and digital sectors must ensure their information and communication technology (ICT) systems can maintain functionality, swiftly recover from disruptions, and remain secure against cyber threats and system failures [7].

The Information Security Unit needs to make sure that MediTrust follows the Digital Operational Resilience Act (DORA) and the Directive on Security of Network and Information Systems 2 (NIS2) to help the company grow in the EU market. These rules say that organization that provide important digital services must have effective cybersecurity governance, operational resilience, and incident reporting systems in place. So, MediTrust must set up rules, ways to keep an eye on things, and ways to run the organization that will let it keep providing healthcare technology services while also being able to stop, find, respond to, and recover from cyber disasters [8].

DORA's operational resilience using MoSCoW requirements

Must have	Should have	Could have	Won't Have
MediTrust must implement ICT risk management frameworks	MediTrust should build redundancy and backup systems	MediTrust could adopt advanced automation for threat detection and operational recovery	MediTrust are not required to eliminate all digital risks but must demonstrate reasonable measures to

			mitigate and manage them.
identify critical digital systems, and ensure continuous monitoring and incident response capabilities	MediTrust should perform scenario-based resilience exercises	MediTrust could enhancing efficiency and response times	
MediTrust must also conduct regular resilience testing and maintain reporting mechanisms for major incidents	MediTrust should Map dependencies across cloud and third-party services to reduce systemic risk		

Table 1 show the MoSCow Requirements for DORA's operational resilience

3.2 NIS2 reporting obligations

Network and Information Systems 2 (NIS2) reporting duties mandate organisation to report substantial cybersecurity incidents to national authorities within designated deadlines, as stipulated by the Directive on Security of Network and Information Systems 2 [7].

NIS2, MediTrust needs to set up clear rules for cybersecurity and a systematic way to report incidents. To lower the chances of cyber incidents, the organization needs to put in place risk management tools including access control, network monitoring, vulnerability management, and supply chain security. MediTrust must tell the right people within the required time range if a major cybersecurity problem happens and keeps them updated on its effects and how it is being dealt with [8].

4.0 Governance & Strategy

Governance and Strategy refer to the way an organization controls, manages, and plans its cybersecurity and information security initiatives to ensure alignment with business objectives, regulatory mandates, and risk management protocols [9].

4.1 Governance Model for MediTrust Based on NIST CSF 2.0

MediTrust Analytics Ltd should use a governance model that is in line with the NIST Cybersecurity Framework to make sure that they handle cybersecurity risks well, follow the rules, and keep sensitive healthcare data safe as they grow into the EU market. The Governance role sets leadership, accountability, and oversight for cybersecurity across the organization. It should be the first part of the governance model. MediTrust should set up a clear governance structure with a Board of Directors, a Chief Information Security Officer (CISO), and a Data Protection Officer (DPO). The CISO and DPO will oversee enforcing policies, managing cybersecurity strategy, and making sure that rules like the General Data Protection Regulation, NIS2 Directive, and Digital Operational Resilience Act are followed. The company should make rules about protecting data, managing AI, keeping the cloud safe, controlling access, and managing third party risks. MediTrust must keep track of important things like patient medical records, AI training datasets, Internet of Things (IoT) medical devices, and its cloud infrastructure.

4.2 Linking Security Strategy to Business Goals

Organization Goal	Security Strategy	NIST CSF 2.0 Function	Benefit to Medi Trust
Expand into EU healthcare market	Set up strong privacy and data security controls	Govern and protect	General Data Protection Regulation and other EU rules are followed [10].
Protect sensitive patient data and AI models	Zero Trust access control, encryption, and a safe cloud design	Protect	Stop data leaks and keep patients' trust [10].
Maintain reliable healthcare services	Monitoring all the time and planning how to handle incidents	Detect and respond	Cyber risks can be found and stopped faster [10].
Manage third party research partners and software dependencies	Managing risks in the supply chain and checking the security of vendors	Identify and govern	Less chance of attacks on the software supply chain [10].
Support hybrid workforce securely	Protect with multi-factor authentication and least-privilege access	Protect	Safe access for remote developer and analysts working from home [10].
Ensure operational resilience	Planning for business survival and disaster recovery	Recover	Providing hospitals and clinics with services all the time [10].

Table 2 show the Security Strategy to Business Goals

5.0 Risk Management

Risk Management is the procedure of identifying, assessing, and reducing cybersecurity threats that may impact an organization systems, data, and operations [12].

5.1 High-level risk assessment focusing on software supply chain risks

MediTrust's significant supply chain risks came from open-source sources that aren't secure and third-party software that has been hacked. These can directly affect the organization's healthcare platforms and AI models, making them less reliable. MediTrust depends on outside libraries, cloud services, and research partners. If these dependencies are weak, attackers could use them to add harmful code, steal private medical data, or mess up clinical systems [11].

MediTrust should follow supply chain security best practices that are in line with the NIST Cybersecurity Framework to lower these risks. These should include dependency scanning, vendor risk management, secure CI/CD pipelines, and ongoing monitoring. Keeping track of software parts and checking AI training datasets will help protect the security of both the development environment and healthcare systems that are already in use [11].

Risk, description, likelihood, impact. Risk level and mitigation control table

Risk	Description	Likelihood	Impact	Risk Level	Mitigation Control
Poisoned AI Training Data	If malicious or hacked datasets are used to teach AI models, they could make biased or dangerous clinical recommendations.	Medium	High	High	Check the validity of sources, set up data provenance tracking, and test the validity of the model [11].
Vulnerable Open-Source Dependencies	There is a chance that third-party tools used in development have known security holes that attackers can use.	High	High	Critical	Keep a Software Bill of Materials (SBOM) and patch libraries daily and use tools that scan for dependencies [11].
Compromised Third-Party Software	Attackers could get into the systems of outside vendors or programming tools and add harmful code to software updates.	Medium	High	High	Check the security of vendors and put in place methods for verifying secure code [11].
Malicious Code Injection in CI/CD Pipeline	Attackers could add bad code to production builds if they get into the development process.	Medium	High	High	Protect CI/CD systems, make sure strong authentication is used,

					and keep an eye on the build process [11].
Insecure Research Partner Access	Researchers from outside the company who access AI data or development systems could add code or data that can't be trusted.	Medium	Medium	Medium	Use Zero Trust entry controls and only let people into isolated areas [11].
Dependency Confusion Attacks	Attackers put out harmful packages with names that sound like internal libraries to get developers to load them.	Medium	High	High	Check the sources of your packages and use private package libraries [11].

Table 3 show the High-level risk assessment and mitigation control

5.2 Cloud Misconfigurations

Cloud misconfigurations are security vulnerabilities that arise when cloud resources such as servers, storage, databases, or applications are improperly or insecurely configured, resulting in unintentional disclosure or access to sensitive data and services [13].

One of the most common ways for companies that use cloud technology to lose data is by setting up the cloud wrong. People who aren't supposed to be there could get to

MediTrust Analytics Ltd's private patient data, AI training datasets, and internal systems if cloud resources are set up incorrectly.

For example, The WS S3 bucket that stores patient data is open to everyone, not just authorised users. This can cause data breaches and not following the rules. These problems happen because access controls aren't set up right, network ports are open, or storage isn't encrypted. These problems can be fixed by requiring least-privilege access, blocking public access, and watching all the time. Zero Trust Can Mitigate Cloud Misconfigurations through continuous verification, limit lateral movement if a misconfiguration exposes one system, automate configuration checks using security as code tools and detect anomalous access or configuration changes in real-time [13].

6.0 Contingency Planning

Contingency planning is the process of making plans and methods for how to keep things running or quickly get them back to normal when something unexpected happens. Cyberattacks, system breakdowns, natural disasters, and data breaches are some of these events [14].

6.1 Disaster Recovery Plan for Ransomware Attack

Infected systems should be quickly found and shut down as part of a disaster recovery plan for a ransomware attack. This will stop the malware from spreading. The incident reaction team should shut down accounts that have been hacked, disconnect servers that are affected, and keep the logs for future investigation.

For Example, MediTrust's cloud-based Git-based source code files and AI training data are locked up by a ransomware attack by this following steps, Attackers secure AI training data and source code that is stored in the cloud for MediTrust. The organization finds strange behaviour and shuts down systems that are affected.

Accounts that have been hacked are locked down, and the incident response process is started to stop the threat from spreading further.

The recovery, MediTrust should separates affected computers, locks down accounts that have been hacked, and starts incident response. IAM takes away tokens and requires MFA. Cloud teams rebuild workloads using secure IaC and recover backups that can't be changed. AI teams check the accuracy of datasets and look for poisoning. Controlled recovery and resilience processes that are in line with Zero-Trust are used to bring services back online [15].

The Cloud Security Architect team should use safe Infrastructure as Code templates to rebuild servers that have been hacked and recovers encrypted datasets from backups that can't be modified and saved in a different cloud location. This is steps called Micro-segmentation rules, and it stop malware from spreading to other workloads [14].

The Zero Trust and IAM Engineering team should takes away access tokens, changes API keys, and makes sure that all protected accounts use multi-factor authentication at the same time [16].

The AI, Data, and Security Division should be checks and make sure that restored AI training datasets are still valid and looks for data poisoning in machine learning operations [15].

As required by EU cybersecurity legislation, the Governance, Risk, and Compliance team writes down what happened, updates the ICT risk record, and alerts the authorities about it [16].

7.0 Protection Mechanisms

Protection mechanisms are the tools and security controls that are used to keep data from being lost, stolen, or accessed by people who aren't supposed to be there. These things help keep systems, networks, and private info safe from harm [14].

7.1 Modern Security Controls

Modern security measures help organization find threats, keep critical information safe, and respond rapidly to cyber incident. Today security controls help Organization find threats early, keep sensitive data safe, and act quickly to cyber incidents. AWS and Azure are just two of the cloud environments that tools like Cloud Security Posture Management (CSPM) constantly check for mistakes, weak rights, or unsafe storage settings that could leave data open or let attackers in. CSPM lets security officers know about these threats right away, which helps stop breaches before they happen [15].

For example, if an AI training data storage bucket is unintentionally made public, CSPM would instantly notify administrators or alter the settings to keep the data from being seen. Security Information and Event Management (SIEM) systems look for strange behaviour by gathering logs from servers, applications, and networks. For example, if someone tries to log in several times and fails, then successfully logs in from an unexpected place, the SIEM sends out an alert for further inquiry [16].

Multi-Factor Authentication (MFA) that is resistant to phishing, such hardware security keys that use FIDO2, makes sure that users must prove their identity in person. This keeps attackers from getting into systems even if they steal passwords [16]

References

- [1] T. Campbell, *Practical Information Security Management: Organizational Security*, Springer, 2021.
- [2] R. von Solms and J. van Niekerk, "From information security to cyber security," *Computers & Security*, vol. 38, pp. 97-102, 2022.
- [3] GDPR, Regulation (EU) 2016/679, "General Data Protection Regulation," European Union, 2023.
- [4] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, NIST Special Publication 800-53 Rev. 5, Gaithersburg, MD, USA, 2021.
- [5] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, NIST Special Publication 800-53 Rev. 5, Gaithersburg, MD, USA, 2021.
- [6] Digital Operational Resilience Act, Regulation (EU) 2022/2554 on digital operational resilience for the financial sector, 2022.
- [7] International Organization for Standardization, ISO/IEC 27001: Information Security Management Systems Requirements, Geneva, Switzerland, 2021.
- [8] National Institute of Standards and Technology, Special Publication 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations, Gaithersburg, MD, USA, 2022.
- [9] National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0*, Gaithersburg, MD, USA, 2024.

- [10] International Organization for Standardization, *ISO/IEC 27001: Information Security, Cybersecurity and Privacy Protection Information Security Management Systems*, Geneva, Switzerland, 2022.
- [11] European Union Agency for Cybersecurity, *Threat Landscape for Supply Chain Attacks*, ENISA, 2023.
- [12] National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations*, NIST SP 800-37 Rev.2, 2021.
- [13] Google Cloud, *Cloud Security Best Practices and Misconfiguration Prevention*, Google Cloud Security Whitepaper, 2023.
- [14] J. López et al., “Enhancing Cloud Security Proactive Threat Monitoring and Detection Using a SIEM-Based Approach,” *Appl. Sci.*, vol. 13, no. 22, p. 12359, 2023.
- [15] S. Reddy Cheruku, “AI-Driven Security Posture Management: A Revolutionary Approach to Multi-Cloud Enterprise Security,” *Int. J. Sci. Res. Computer Science. Eng. Information. Technology*, vol. 11, no. 1, pp. 497-509, Jan. 2025.
- [16] P. Kumar, “Next-generation secure authentication and access control architectures,” *Int. J. Computer. Exp. Sciencie. Eng.*, vol. 11, no. 3, pp. 4966-4995, 2025.