

Assignment – Research and case scenario in Data Security and Compliance

Ben Roberts (2205382)

Data Security and Compliance (FT - ACCA5034)

University of Wales Trinity Saint David – School of Applied Computing

Table of Contents

Table of Contents.....	2
Introduction.....	4
Task 1 - Research in Data Security and Compliance.....	5
Zero Trust.....	5
Principles of Zero Trust.....	5
Implementation Challenges.....	8
Efficacy compared to traditional perimeter-based models.....	10
Task 2 – Case Scenario.....	11
Assumptions.....	11
Data Security Programme.....	12
Introduction.....	12
Purpose.....	12
Scope.....	12
Principles, Governance and Strategy.....	12
Organisational Structure.....	13
Cloud Security Architect.....	13
DevSecOps Lead.....	14
Risk Assessment & Disaster Recovery Manager.....	14
Compliance Officer.....	14
Cybersecurity Manager.....	14
Employee Requirements.....	14
Password Policy.....	15
Device Policy.....	15
Risk Management Policy.....	16
Disaster Recovery Policy.....	17
EU Compliance Requirements.....	17
Protection Mechanisms.....	18
Conclusion.....	19
References.....	20

Table of Figures

Figure 1: Diagram demonstrating the benefits of using a Zero Trust network when compared to conventional security architectures [1].....	5
Figure 2: Example diagram of a Zero Trust Implementation Framework [2].....	6
Figure 3: Table showing a number of cybersecurity domains with potential benefits and limitations of certain kinds of Zero Trust implementations, from [3].....	9
Figure 4: Table showing the cost of various Zero Trust services in 2022, from [4].....	9
Figure 5: Diagram from the NIST Cybersecurity Framework [5].....	13
Figure 6: Table of CSF Core Functions [5].....	14

Introduction

This document covers a number of topics relating to Data Security and Compliance, primarily relating to Zero Trust.

The first section of this document covers a comprehensive research and analysis of Zero Trust, its principles as outlined by the NCSC and a variety of other topics associated with Zero Trust.

The second section (Task 2) composes a data security programme for a theoretical organisation in accordance with regulations and Zero Trust security policies based upon the findings from Task 1 as well as personal experience.

Task 1 - Research in Data Security and Compliance

Zero Trust

Zero Trust is a security architecture that assumes no implicit trust is granted to users [6]. The Zero Trust Architecture is built upon the principles of least privileges, specifically scoped and user-specific access controls, and stringent policy enforcement that only provides users and devices with permissions that are required for them to work, regardless of location and/or standing [7]. Zero Trust was introduced to account for the fact that traditional cybersecurity models are unable to safely accommodate remote working and bring your own device (BYOD) policies [8] and moves the focus of security from the network perimeter to individual assets [9].

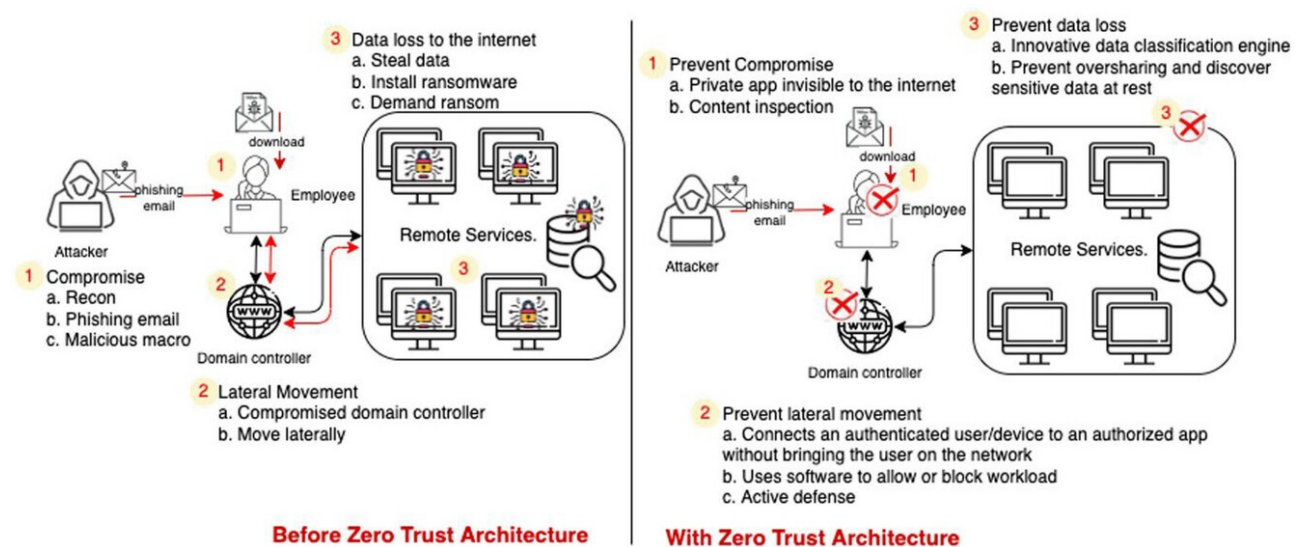


Figure 1: Diagram demonstrating the benefits of using a Zero Trust network when compared to conventional security architectures [1]

Zero Trust is an effective security measure because its access controls reinforce systems against data breaches and the segmentation of the network limits the spread of malware [10]. This can have significant advantages in the long term, such as significant cost savings afforded by reduced insurance fees and lowered risks of a cybersecurity breach [11].

Principles of Zero Trust

The UK National Cybersecurity Centre [12] defines the eight principles of Zero Trust as:

1. Knowing the architecture, including users, devices, data and services on the network.
2. Knowing the identities of users, services and devices.

3. Assessing user behaviour as well as device and service health.
4. Utilising policies for request authorisation.
5. Requiring authentication and authorisation for all parts of the network.
6. Monitoring users, devices and services.
7. Not trusting any network, even the network being secured.
8. Primarily utilising services designed around Zero Trust.

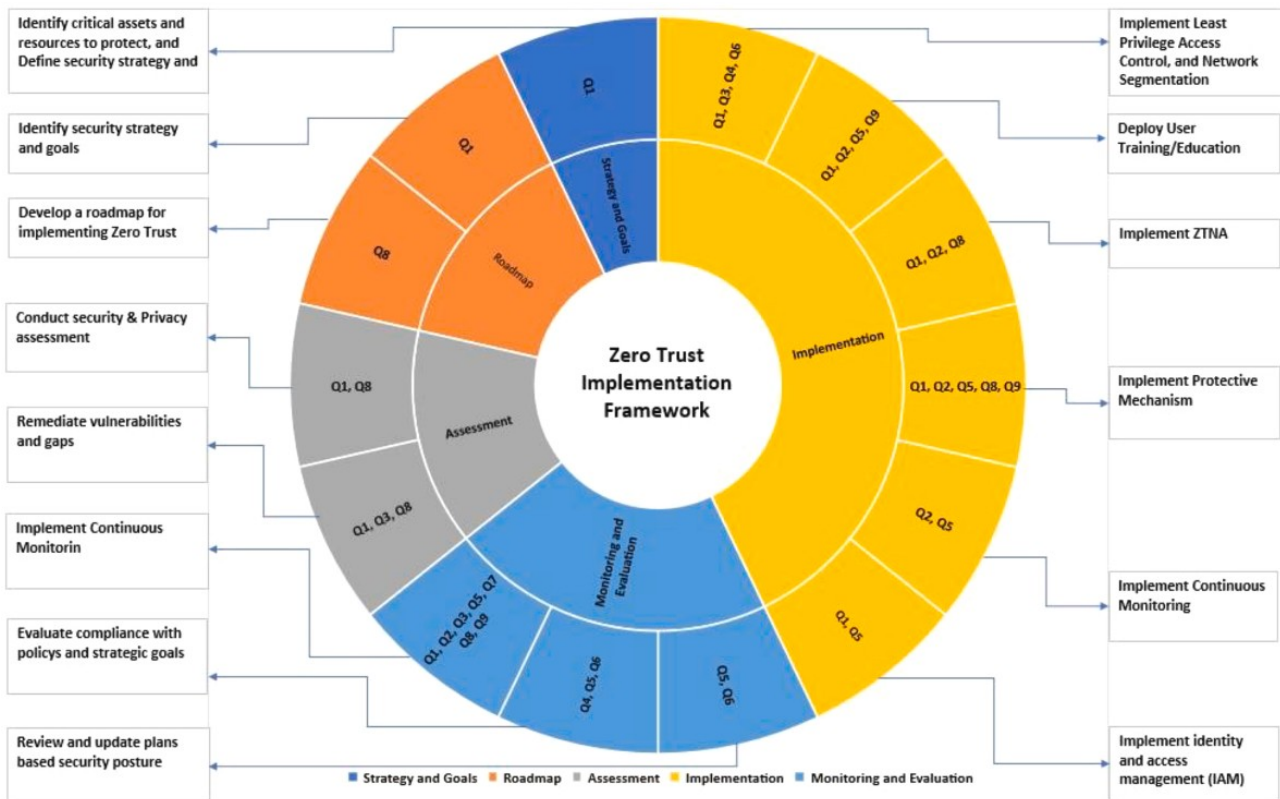


Figure 2: Example diagram of a Zero Trust Implementation Framework [2]

As an important part of Zero Trust is knowing the overall network architecture. This will involve an asset discovery phase to make note of every device that will be used on the network and what levels of trust will be required for them to function [13]. For example, in a bring your own device setup it would be preferable to give external devices lower access privileges [14]. It is also possible to use stricter forms of authentication to ensure device security, such as ones based on a blockchain [15].

Maintaining the knowledge of users services and devices is also essential to a Zero Trust architecture. This usually comes in the form of an authentication system. Under the standard castle-and-moat networking model, single sign-on (SSO) is commonly used as it provides a convenient way for users to access all the necessary resources. However, this approach is fundamentally incompatible with Zero Trust principles as it requires re-use of authentication certificates which attackers can easily compromise [16].

Ensuring the security of a Zero Trust network requires constant scanning and evaluation of device and service health [17]. As an example, a zero trust network will need to ensure that every device has been updated to the latest software versions so that any potential security vulnerabilities have been patched [18].

The most essential component of the Zero Trust architecture is that it is built upon the principle of least privilege, which is defined as only permitting a user to do what is absolutely required to perform their required tasks [19].

If a user account or external software is not correctly configured for minimum privileges, it may expose potential security issues due to higher-than-necessary privilege configurations [20]. For example, if a standard user had administrator rights on a workstation then they would be able to run unauthorised software that could perform dangerous modifications at a low level.

Zero trust is heavily reliant on strict authentication requirements. These can include mandating passwords of a minimum strength and/or requiring users to perform two-factor authentication and the use of biometric authentication [21]. Use of two-factor authentication is commonly advised as it provides an additional layer of security [22]. Examples of two factor authentication include knowledge-based methods such as a secret question, ownership-based methods such as a physical token or a mobile device or inherence-based methods which are based on biometrics [22].

In some zero trust networks, passwordless authentication with biometrics is used instead of passwords as it has a similar level of security without requiring users to remember complicated passwords [21].

Furthermore, a zero trust network will need to have an intrusion detection system configured in order to prevent unauthorised access so that it can remain fully secured [23].

Another example of a network security feature that can be used in a network would be firewalls. Firewalls can be used to filter incoming and outgoing packets to and from certain domains. However, traditional firewall systems that rely on static rules are incompatible with zero trust principles due to them being harder to use across domains so a decentralised model based on encrypted tokens can be used instead [24].

In a Zero Trust architecture, it is imperative to assume that the network is always at risk, and that attacks can and will occur [25].

For example, virtual private networks (VPNs) are commonly used to allow external access to a network from a remote location. However, VPNs implicitly trust all incoming connections and allow full access to a network which is incompatible with Zero Trust principles [26]. Utilising a Zero Trust Network Access (ZTNA) solution is preferred because it aligns better with Zero Trust principles by enforcing constant verification [27]. End-to-end encryption may also be used to ensure that data is secured against interception. [26]

Finally, Zero Trust networks must utilise software and services that can function as intended in a Zero Trust environment. It is preferable to use services that use interoperable open standards instead of ones that are reliant on proprietary mechanisms [28].

In some instances an organisation will have to use a legacy service that has not been or is no longer being updated to support Zero Trust [29].

Implementation Challenges

Despite the significant benefits of using a Zero Trust Architecture, there are multiple challenges that arise when trying to implement it. The extremity of these issues is variable based on the size of an organisation, the resources they have access to and any existing infrastructure that they may have [2]. Most notably, there are few standardised ZTA frameworks which means that many organisations will have to create their own framework [3]. Zero Trust networks are also difficult to deploy and will require trained security personnel to properly implement and maintain [30]. ZTA may require hiring a Zero Trust consultant which may be costly.

Domain	Key Focus Areas	Strengths (✓)	Common Limitations (✗)	Representative Studies
Cloud Computing	Microservices, containerization, remote access	✓ Access control ✓ Identity verification ✓ Network segmentation	✗ Limited orchestration ✗ Weak auditing ✗ Environmental perception often missing	D'Silva et al. [24], Liu et al. [71], Zhang et al. [23]
Internet of Things (IoT)	Scalability, resource constraints, edge computing	✓ Dynamic trust engines ✓ Context-aware access ✓ Network segmentation	✗ Weak cryptography ✗ Rare use of orchestration ✗ Minimal auditing	Ameer et al. [3], Huber & Kandah [13], Tao et al. [8]
Healthcare Systems	EHRs, medical IoT, compliance	✓ Secure remote access ✓ ML-based detection ✓ Attribute-based access control	✗ Poor device-level segmentation ✗ Limited cryptographic adaptation ✗ Manual orchestration	Alshaikh et al. [62], ElSayed et al. [5]
AI/ML Systems	Model protection, dynamic policy, autonomous decisions	✓ Behavioral monitoring ✓ Risk-adaptive access ✓ Identity validation	✗ Lacks explainability ✗ Vulnerable models ✗ Missing lifecycle audits	Abbas et al. [20], Rakhshani et al. [19], Xing et al. [21]
Blockchain-based Systems	Decentralized policy enforcement, trust anchors	✓ Tamper-proof logs ✓ Smart contract enforcement ✓ Identity immutability	✗ High latency ✗ Off-chain dependency ✗ Privacy trade-offs	Gigli et al. [18], Wu et al. [10]
Industrial and Mobile Networks	Real-time processing, device mobility, automation	✓ Strong segmentation ✓ Access enforcement at edge ✓ Trust propagation	✗ Low orchestration ✗ Legacy system integration ✗ Limited environmental modeling	Xing et al. [21], Fang et al. [10], Jing et al. [15]

✓ indicates that the dimension is fully addressed and ✗ indicates that the dimension is not addressed.

Figure 3: Table showing a number of cybersecurity domains with potential benefits and limitations of certain kinds of Zero Trust implementations, from [3]

Implementing a Zero Trust Architecture is lengthy, expensive and cumbersome [31]. The cost of setting up a Zero Trust implementation is proportional to the size and complexity of an organisation's network, especially if an organisation has multiple facilities and/or needs to work across organisational boundaries [4].

Tools and Resources	ZTA Component	Unit Cost (u) per Year	ZTA tool cost based on the number of employees in an organization			
			1 - 100	101 - 400	401 - 700	701 - 999
CylancePROTECT for Endpoint Protection Cylance (2022)	Subject and Resources	\$45 per endpoint for 1-250 endpoints. \$41.75 per endpoint for 501 - 1000 endpoints	\$4,500.00	\$16,700.00	\$29,225.00	\$41,708.25
Kaspersky Security for Business with encryption services AO Kaspersky Lab, 2022	Data Encryption - Subject, Resources, and PEP Endpoint Protection - Subject and Resources	\$45 per node	\$4,500.00	\$18,000.00	\$31,500.00	\$44,955.00
Google Workspace for Cloud-based Storage and Access Control Prokopets (2022)	Access Control - PE in PDP Data Encryption - Subject, Resources, and PEP					
Cloud Storage - Resources	2TB pooled cloud storage for \$96 per user	\$9,600.00	\$38,400.00	\$67,200.00	\$95,904.00	
Microsoft OneDrive Prokopets (2022)	Access Control - PE in PDP Data Encryption - Subject, Resources, and PEP Cloud Storage - Resources	1 TB for \$60 per user	\$6,000.00	\$24,000.00	\$42,000.00	\$59,940.00
Virtru Encryption Virtru Team, 2021	Subject, Resources, and PEP	\$948 per 5 user	\$18,960.00	\$75,840.00	\$132,720.00	\$189,410.40
Microsoft Azure Active Directory for Access Control Zelleke (2021)	PE in PDP	Comes free with Microsoft OneDrive or \$72 per user separately	\$7,200.00	\$28,800.00	\$50,400.00	\$71,928.00
Security Engineer Salary.com, 2022	PA in PDP	\$60 per hour	5h/week \$14,400.00	10h/week \$28,800.00	20h/week \$57,600.00	30h/week \$86,400

Figure 4: Table showing the cost of various Zero Trust services in 2022, from [4]

In a systematic literature review on the implementation challenges of Zero Trust, it was found that different fields and domains have differing requirements for a Zero Trust network implementation. While Zero Trust is incredibly important in Cloud Computing due to the inadequacies of traditional perimeter-based models, cloud infrastructure often requires strict management and arrangement of microservices as well as strict compliance requirements and granular access controls. It was found that many proposed Zero Trust models lack the essential orchestration component for proper management in a cloud environment. [3]

The Internet of Things (IoT) has become increasingly important for modern networks, but many IoT devices often have poor default credentials and weak hardware capabilities which can often make strict Zero Trust requirements harder to implement. These issues are further compounded when many IoT devices are on a network due to the strict real-time requirements that may be imposed. While there are methods of optimising, such as using a trust engine, many Zero Trust implementations do not include them. [3]

Mobile technologies are also a notable component of modern industrial networks, but mobile devices frequently pose a potential threat to the network. In many cases these industrial mobile devices will commonly run into compatibility issues (such as when an older device is not compatible with fast 5G networks that are capable of low-latency policy enforcement), are hard to manage and often have isolated audit logs [3].

Furthermore, migrating an existing network to a Zero Trust architecture is much more difficult than building a new Zero Trust network from scratch. While a hybrid approach combining Zero Trust principle a legacy model is possible [32], it may still require a lengthy and expensive auditing process.

Even if it is cheaper than fully converting a network to Zero Trust, a hybrid Zero Trust approach does still have a number of drawbacks. These include much higher communications latency, increased network complexity and higher operational overhead [33].

Because of the changes made for security, implementation of a Zero Trust Architecture can also impede productivity as users will generally find Zero Trust inconvenient [22].

Certain approaches that increase user convenience, such as single-sign on, are fundamentally incompatible with Zero Trust which can lead to reduced productivity.

Zero Trust networks may also run into compatibility issues with legacy services and technologies that predate the general adoption of Zero Trust. While many systems and services can be patched to properly support Zero Trust, certain services that are essential to an organisation's workflow may no longer be supported. In many cases these services can be isolated from the rest of the network (or even be kept offline entirely, such as for computers running older operating systems solely for the purposes for controlling older machinery), but there may be cases where these systems can not be kept offline and will instead have to be decommissioned in favour of a more up-to-date service. [34]

Beyond these implementation issues there are also a number of threats that can be exposed to a Zero Trust network. An example of these potential threats would be a denial of service attack against an essential network service required to keep the trust system intact [32].

Efficacy compared to traditional perimeter-based models

The traditional network model is to use a perimeter-based system wherein incoming connections must be authenticated and all devices within the network are considered to be trusted by default. Furthermore, once authenticated a connection will remain trusted within a perimeter-based network. This means that malicious objects can move laterally across the network whilst only having to authenticate once [35]. By comparison, a properly-implemented Zero Trust Architecture can effectively mitigate any potential lateral movement that can occur within a traditional perimeter-based network. [36]

Because Zero Trust principles are built upon constant verification and omitting implicit trust, this enables a network using a Zero Trust architecture to better support external devices inside of the network whilst minimising the potential risks of BYOD [9]. This may allow an organisation to save on spending for internal hardware. It may also reduce the potential blast radius of phishing attacks by explicitly limiting what can be done with stolen credentials.

While it is less secure in principle, the traditional perimeter-based model does hold some niche advantages over a Zero Trust implementation. As an example, Zero Trust network security models lack the standardisation of traditional perimeter-based networks which may mean that a perimeter-based model is better suited for situations where legacy and/or proprietary technologies absolutely must be used [37]. A Zero Trust Architecture may also be less important for smaller networks with a very small number of devices connected, although in those cases it would also be optimal to redesign the network for Zero Trust when expansion is considered.

Task 2 – Case Scenario

Assumptions

As the company is theoretical, it is expected that the organisation can afford to have a number of staff members within its security team and also that it can afford to lease a number of devices to employees. In a more realistic scenario the organisation may have to utilise a BYOD policy due to budgetary restrictions, although in this case such a policy has been disregarded due to trust and security concerns.

The purpose of this section is to design a security programme for a theoretical organisation that sells security and threat analysis services.

Data Security Programme

Introduction

This is a Zero Trust-aligned data security programme for ResilientIntellect Ltd. (hereafter referred to as “the organisation”).

This document is fully subject to change, and all stakeholders and employees are expected to remain up to date whenever it is altered.

Purpose

As an organisation operating within the cybersecurity sector, the organisation must ensure maximum protection of sensitive and confidential data at risk of significant reputational damage. This policy aims to achieve full alignment with Zero Trust principles to support a fully hybrid workforce.

Scope

This programme covers a number of areas of the organisation’s infrastructure such as compliance, employee requirements and system configuration. This programme should be considered subject to change as security practices may change in the future as newer, more dangerous threats arise.

In the event that a specific business need is identified that may have to be exempted by any of the policies outlined in this security programme (be it due to cost, complexity, negatively affecting other business needs, etc.) a risk assessment must be performed by a cybersecurity manager.

Principles, Governance and Strategy

This entire policy is intended to align with Zero Trust Principles, as defined by the NIST Cybersecurity Framework 2.0 [5]. The CSF is considered the primary source to use for Zero Trust and is therefore the leading basis of this programme.



Figure 5: Diagram from the NIST Cybersecurity Framework [5]

The core outcome of this policy is to provide a Zero Trust compliant document, as outlined by the CSF Core Functions.

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Figure 6: Table of CSF Core Functions [5]

In short, the core principle of Zero Trust is to “never trust, always verify” and as such this programme is built with maximising security potential even in cases where it may appear inconvenient to do so. Access is strictly enforced through means of authentication and the organisation intends to minimise risks wherever can be necessary.

Organisational Structure

The following roles within the organisation are mandatory for operation and should ideally be filled whenever possible.

Cloud Security Architect

The role of the Cloud Security Architect is to ensure that the organisation’s cloud platforms are correctly configured for maximum privacy and security. Their responsibilities include:

- Ensuring maximum security within cloud configurations where possible
- Collaborating with teams, clients and other individual to maintain effectiveness and good practice

- Collaborate with the Compliance Officer to ensure compliance on the technical side

DevSecOps Lead

The organisation uses a DevSecOps development model, which focuses on the security approach of the product provided to clients. The DevSecOps lead therefore has the following roles [38]:

- Leading DevSecOps
- Co-ordinate the development, security and operations teams
- Manage security-focused continuous integration and delivery pipelines

Risk Assessment & Disaster Recovery Manager

As the organisation must process a lot of sensitive data, it is imperative that a risk assessment and disaster recovery manager handles the process of preparing for and recovering from any potential threats that emerge. This manager has the following roles:

- Regularly conduct risk assessments
- Maintaining a disaster recovery plan
- Co-ordinate disaster recovery efforts in the event of a breach and/or major data loss

Compliance Officer

Cybersecurity often involves a large number of regulations, some of which may be region-specific. A compliance officer is essential to minimise organisational risk from litigation and cybersecurity risks, and has the following roles:

- Remain up to date with and ensure compliance with all relevant regulations such as NIS2, DORA and GDPR for European expansion.
- Monitor and ensure that the wider staff are remaining within organisational compliance regulations.
- Routinely inspect all facets of the organisation for compliance issues, and organise training in cases where compliance may be substandard.

Cybersecurity Manager

The purpose of this Cybersecurity Manager role is to manage all facets of the organisation's general cybersecurity approach, and as such has the following roles:

- Audit and update the organisation's security policy
- Authorise potential exceptions to the policy in cases where a business need is required
- Co-ordinate all other cybersecurity personnel

Employee Requirements

While technical means can be used to ensure against potential security problems, there are also issues that can arise when users are acting outside of secure protocol. Therefore, employees must abide by the following terms:

1. All employees must complete a zero trust awareness training program to ensure that they are familiar with all the security processes required of them.

2. Distribution of confidential data belonging to outside sources of any kind is not permitted under any circumstances via any means, be they digital, physical or word-of-mouth.
3. All user passwords must be unique, not used for multiple services (be they personal or associated with the organisation) and in keeping with the organisation's password policy as outlined below.
4. Furthermore, a phishing-resistant form of multi-factor authentication (MFA), such as biometrics, time-based one-time password protection (TOTP), physical FIDO2 authentication keys or other means authorised by the organisation must be used as a layer of protection in the event that a password is figured out. Methods of MFA which are inherently vulnerable to phishing (such as SMS or email codes) are not permitted, nor are single-factor passwords or passkeys.
5. If a work device containing essential data is lost or damaged, the administrators must be contacted immediately.
6. Upon termination, employees must return all confidential documents. Furthermore, any non-essential data saved to their accounts will be permanently deleted.

Password Policy

Because passwords are essential for gaining access to a system, all passwords used on the organisation's system must meet these stringent requirements as a weak password can jeopardise the whole system.

1. Passwords must be at least 32 characters long and contain at least one of all the following:
 - Alphanumeric characters
 - Numbers
 - Uppercase and lowercase characters
2. Furthermore, passwords containing names or dictionary words are not permitted as those are inherently more vulnerable to cracking attempts.
3. Passwords must also be changed in the event that any suspected security issues arise, such as a suspected leak of authentication details zero-day vulnerability being found in the organisation's software stack.

It is recommended that employees update their passwords regularly, although the organisation does not mandate password changes as those lead to diminishing returns [39].

Device Policy

This organisation uses a hybrid workforce, which means devices must be configured to work securely both inside and outside of the organisation's perimeter.

1. Only devices which are formally owned by the organisation may be used to access organisational data. For remote work, a company device will be leased and will provide remote access via Zero Trust Network Access (ZT-NA). Furthermore, unauthorised devices may not be connected to the organisation network and will be blocked.

2. Unencrypted external data storage devices that lack authorisation from the organisation may not be connected, and mounting them will be blocked in order to prevent data leakage.
3. The only operating system permitted on corporate devices is the organisation's internal flavour of Debian Linux. Microsoft Windows is not permitted on the network as it has infamously poor security.
4. BIOS/UEFI access is to be locked where possible and secure boot must be enabled to allow for the full drive encryption part of this policy to function as intended.
5. Web browsers installed on computers must be configured to block cookies, browser scripts and advertisements as those provide a significant security and privacy risk. User accounts must be automatically logged out after five minutes of inactivity to prevent unauthorised access. Users are encouraged to log out earlier than that if planning to leave the computer unattended for any reason.
 - a. For this reason, organisation devices must all have internal TPM2 adapters.
6. The use of owned devices (such as laptops and mobile phones) not associated with and unowned by the organisation is not permitted on the corporate network.
 - a. Exceptions can be made in situations wherein it would be feasibly impossible to work otherwise (such as in cases where specific accessibility hardware is required). Such exceptions should be approved by a cybersecurity manager.
7. All hard drives are to be partitioned with Linux Unified Key Setup (LUKS) and a hardware-accelerated TPM2 configuration for full drive encryption.
 - a. Should a better option emerge, consider re-partitioning devices if possible.

Risk Management Policy

It is impossible to completely eliminate risk even in a Zero Trust setup. However, many steps can be taken to minimise potential risk where possible. The Risk Assessment & Disaster Recovery manager shall update this section of the policy as necessary. The basis of this policy draws from by the "Orange Book Management of Risk" document published by the UK government [40].

1. The process of risk management is treated as essential to all employees in leadership positions, and is to be considered an integral component of all organisational activities.
 - a. This risk management process is also expected to be collaborative and cross-departmental.
2. Risks must be strictly identified before doing anything. This identification process m
 - a. If in doubt, do not go ahead with anything if the level of risk cannot be accurately determined.
3. Risk treatment should generally favour safety where possible.
4. To minimise the risk of the artificial intelligence models used by the organisation being compromised ("AI model poisoning"), any AI workflows running within the organisation may not have access to the internet and may not access sensitive information. Training data must also be rigorously checked for potential biases that may cause the AI models to malfunction.
5. While modern software is inherently reliant on dependencies, use of dependencies should be minimised wherever possible as there may be issues further up the dependency chain.

Disaster Recovery Policy

Even with high-level risk management procedures it is still entirely possible that a disaster may occur. Therefore, contingency plans must be put in place to recover in an emergency.

1. System backups must be produced on a weekly basis as so to roll back in the event that a major system becomes nonfunctional. These backups must be kept for at least twelve months at minimum and should ideally be recorded to multiple formats, such as linear tape and/or optical media. These backups must also be heavily encrypted to deter theft. The following data must be backed up where possible:
 - a. Entire system images of major essential systems
 - b. Sensitive business information
 - c. Customer data
 - d. Documents stored on the organisation's internal hosted cloud storage
2. Should a system rollback be required, start with the newest backup and keep going back until a non-compromised version is found.
3. In the event that malware is found to have breached past authentication requirements, immediately deactivate all connections (internal and external) until affected machines have been properly secured.
4. Network design should be constructed around redundancy in order to keep functioning in the event of a disaster. Servers should be equipped with additional Ethernet NICs and should have multiple outgoing ISP connections.

EU Compliance Requirements

In order to operate within the European Union, the organisation must be compliant with the Network and Information Systems directive (NIS2) and the Digital Operational Resilience Act (DORA). As well as being required to operate in the EU, many of these regulations functionally appear to be considered good practice and will therefore be enforced across all branches.

1. In the event of a suspected security breach, the relevant authorities must be contacted immediately and a detailed assessment must be assembled within 72 hours of the suspected breach.
2. Full Drive Encryption must be enabled on all devices. Please see the device policy above for more information.
3. Unnecessary risks within the Zero Trust system must be avoided where possible to maintain a low appetite for risk.
4. Stockholders and employees at board level must accept responsibility for any security breaches.
5. Individuals must act in accordance with the organisation's risk management policy at all times.
6. All personnel must be informed of their security responsibilities within the organisation.
7. Digital operational resilience testing must be performed on a routine basis. As outlined by Article 25 of the European Union Digital Operational Resilience Act [41], this includes but is not limited to:
 - a. Vulnerability assessments of hardware and software.
 - b. Gap analysis of actual system security performance when compared to desired security performance.
 - c. Physical security analysis of computing equipment by ensuring that they have not been opened up or tampered with.

- d. Source code reviews for both organisation software and other open source tools that the organisation relies on.
 - For this reason, proprietary software whose source code is not legally possible to access is to be avoided where possible as it cannot be audited for security.
- e. Assessments of Zero Trust network security to ensure that there are no unsecured endpoints.
- f. Penetration testing of the organisation's security systems.
- g. Compatibility testing with all systems

Protection Mechanisms

Electronic protection mechanisms must also be configured on as many endpoints and cloud systems as possible to maximise security.

1. A Cloud Security Posture Management (CSPM) solution must be implemented across all of the organisation's cloud infrastructure to properly assess resources and ensure secure configurations in addition to automatically prioritising certain risks by severity and issue remediation [42].
 - a. Furthermore, any cloud products that the organisation provides must also be designed to function within other organisation's CSPM setups.
2. A Security Information Event Management (SIEM) system must also be configured in order to have per-device telemetry which can present and manage necessary cybersecurity data for ensuring the organisation's security with real-time alerts [43].
3. Automated Endpoint Detection and Response (EDR) systems will also need to be configured on every endpoint possible for continual monitoring. These EDR systems must also have automatic response set up and should constantly scan for threats including but not limited to malware, phishing and unauthorised access. These EDR systems should also preferably be integrated with the organisation's setup.

Conclusion

In conclusion, a lot of concepts covered within this document detail a number factors related to cybersecurity and compliance, most notably Zero Trust. The example cybersecurity programme uses the research covered in the first task, in addition to independent research based upon existing papers, websites and reports, to come to the best conclusion from what was provided in the brief.

Had this been a live situation, the writer may have had to investigate further into the nuances of the required system and may have also had to perform additional compromises within the policies and tailor them for specific scenario.

References

- [1] P. Phiayura and S. Teerakanok, 'A Comprehensive Framework for Migrating to Zero Trust Architecture', *IEEE access*, vol. 11, pp. 1–1, 2023, doi: 10.1109/ACCESS.2023.3248622.
- [2] C. Itodo and M. Ozer, 'Multivocal literature review on zero-trust security implementation', *Computers & security*, vol. 141, pp. 103827–, 2024, doi: 10.1016/j.cose.2024.103827.
- [3] S. Mushtaq, M. Mohsin, and M. M. Mushtaq, 'A Systematic Literature Review on the Implementation and Challenges of Zero Trust Architecture Across Domains', *Sensors (Basel, Switzerland)*, vol. 25, no. 19, pp. 6118–, 2025, doi: 10.3390/s25196118.
- [4] Z. Adahman, A. W. Malik, and Z. Anwar, 'An analysis of zero-trust architecture and its cost-effectiveness for organizational security', *Computers & security*, vol. 122, pp. 102911–, 2022, doi: 10.1016/j.cose.2022.102911.
- [5] National Institute of Standards and Technology, 'The NIST Cybersecurity Framework (CSF) 2.0', National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 29, Feb. 2024. doi: 10.6028/NIST.CSWP.29.
- [6] J. B. Michael, G. C. Dinolt, F. B. Cohen, D. Wijesekera, and J. B. Michael, 'Can You Trust Zero Trust?', *Computer (Long Beach, Calif.)*, vol. 55, no. 8, pp. 103–105, 2022, doi: 10.1109/MC.2022.3178813.
- [7] D. Pizio and M. Spencer, 'The volatility of trust: Zero Trust and Distributed Trust as “post-trust” cybersecurity models', *Information, communication & society*, pp. 1–18, 2025, doi: 10.1080/1369118X.2025.2507685.
- [8] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, 'Zero Trust Architecture', National Institute of Standards and Technology, NIST Special Publication (SP) 800-207, Aug. 2020. doi: 10.6028/NIST.SP.800-207.
- [9] Ozkaya Erdal and Diogenes Yuri, *Cybersecurity - Attack and Defense Strategies: Improve Your Security Posture to Mitigate Risks and Prevent Attackers from Infiltrating Your System*, Third edition. in Expert insight. Birmingham, England: Packt Publishing Ltd., 2022.
- [10] C. Buck, C. Olenberger, A. Schweizer, F. Völter, and T. Eymann, 'Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust', *Computers & security*, vol. 110, pp. 102436–, 2021, doi: 10.1016/j.cose.2021.102436.
- [11] A. Poirrier, L. Cailleux, and T. Heide Clausen, 'Is Trust Misplaced? A Zero-Trust Survey', *Proceedings of the IEEE*, vol. 113, no. 1, pp. 5–39, 2025, doi: 10.1109/JPROC.2025.3555131.
- [12] 'Zero trust 1.0'. Accessed: Oct. 29, 2025. [Online]. Available: <https://www.ncsc.gov.uk/blog-post/zero-trust-1-0>
- [13] 'Asset management'. Accessed: Nov. 10, 2025. [Online]. Available: <https://www.ncsc.gov.uk/guidance/asset-management>
- [14] 'Bring your own device (BYOD)'. Accessed: Feb. 19, 2026. [Online]. Available: <https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device>
- [15] J.-J. Huang, Z.-Y. Lin, N.-W. Lo, and S.-F. Feng, 'Dynamic trust management framework using blockchain for zero-trust-based authentication in BYOD environments', *Enterprise information systems*, vol. 19, no. 1–2, 2025, doi: 10.1080/17517575.2025.2457952.
- [16] *Zero Trust Technology Integration Issues*. Institute for Defense Analyses, 2022.

- [17] A. Alagappan, S. K. Venkatachary, and L. J. B. Andrews, 'Augmenting Zero Trust Network Architecture to enhance security in virtual power plants', *Energy reports*, vol. 8, pp. 1309–1320, 2022, doi: 10.1016/j.egyr.2021.11.272.
- [18] '3. Assess user behaviour, service and device health'. Accessed: Feb. 20, 2026. [Online]. Available: <https://www.ncsc.gov.uk/collection/zero-trust/architecture-design-principles/assess-user-behaviour-service-and-device-health>
- [19] X. Ma, R. Li, Z. Lu, J. Lu, and M. Dong, 'Specifying and enforcing the principle of least privilege in role-based access control', *Concurrency and computation*, vol. 23, no. 12, pp. 1313–1331, 2011, doi: 10.1002/cpe.1731.
- [20] Michael E. Whitman and Herbert J. Mattord, *Principles of Information Security*, 7th Edition. Cengage Learning, 2021. Accessed: Nov. 19, 2025. [Online]. Available: <https://www.cengage.uk/c/principles-of-information-security-7e-whitman-mattord/9780357506431/?searchISBN=9780357506431>
- [21] Q. Shen and Y. Shen, 'Endpoint security reinforcement via integrated zero-trust systems: A collaborative approach', *Computers & security*, vol. 136, pp. 103537-, 2024, doi: 10.1016/j.cose.2023.103537.
- [22] K. Marky *et al.*, "'Nah, it's just annoying!'" A Deep Dive into User Perceptions of Two-Factor Authentication', *ACM transactions on computer-human interaction*, vol. 29, no. 5, pp. 1–32, 2022, doi: 10.1145/3503514.
- [23] V. Sobchuk, R. Pykhnivskiy, O. Barabash, S. Korotin, and S. Omarov, 'SEQUENTIAL INTRUSION DETECTION SYSTEM FOR ZERO-TRUST CYBER DEFENSE OF IOT/IIOT NETWORKS', *Сучасні інформаційні системи*, vol. 8, no. 3, pp. 92–99, 2024, doi: 10.20998/2522-9052.2024.3.11.
- [24] Dr Daniel Díaz-Sánchez, Dr Florina Almenarez-Mendoza, Dr Celeste Campo-Vázquez, and Dr Carlos García-Rubio, 'Zero-trust token authorization with trapdoor hashes for scalable distributed firewalls', *Future generation computer systems*, vol. 176, pp. 108227-, 2026, doi: 10.1016/j.future.2025.108227.
- [25] *Five Foundational Elements of a Zero Trust Enterprise*. Institute for Defense Analyses, 2021.
- [26] S. M. Zohaib, S. M. Sajjad, Z. Iqbal, M. Yousaf, M. Haseeb, and Z. Muhammad, 'Zero Trust VPN (ZT-VPN): A Systematic Literature Review and Cybersecurity Framework for Hybrid and Remote Work', *Information (Basel)*, vol. 15, no. 11, pp. 734-, 2024, doi: 10.3390/info15110734.
- [27] Syed Hasnat Ansar, Arslan Sadiq, Uswa Ihsan, Humaira Ashraf, and Somantri, 'Fortifying Linux Server and Implementing a Zero Trust Network Access (ZTNA) for Enhanced Security', *Engineering proceedings*, vol. 107, no. 1, pp. 99-, 2025, doi: 10.3390/engproc2025107099.
- [28] 'Zero trust architecture design principles'. Accessed: Nov. 05, 2025. [Online]. Available: <https://www.ncsc.gov.uk/collection/zero-trust/architecture>
- [29] 'Obsolete products'. Accessed: Feb. 23, 2026. [Online]. Available: <https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/obsolete-products>
- [30] M. Klesiewicz, 'The hidden dangers of sudo: security-oriented analysis of misconfigurations', *J Comput Virol Hack Tech*, vol. 22, no. 1, p. 10, Dec. 2025, doi: 10.1007/s11416-025-00590-0.
- [31] A. M. Abdelmagid and R. Diaz, 'Zero Trust Architecture as a Risk Countermeasure in Small–Medium Enterprises and Advanced Technology Systems', *Risk analysis*, vol. 45, no. 8, pp. 2390–2414, 2025, doi: 10.1111/risa.70026.
- [32] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, 'Zero Trust Architecture', National Institute of Standards and Technology, NIST Special Publication (SP) 800-

207, Aug. 2020. doi: 10.6028/NIST.SP.800-207.

- [33] M. Hashem Eiza, B. Akwiry, A. Raschella, M. Mackay, and M. K. Maheshwari, 'A Hybrid Zero Trust Deployment Model for Securing O-RAN Architecture in 6G Networks', *Future internet*, vol. 17, no. 8, pp. 372-, 2025, doi: 10.3390/fi17080372.
- [34] G. M. Køien, 'Zero-Trust Principles for Legacy Components: 12 Rules for Legacy Devices: An Antidote to Chaos', *Wireless personal communications*, vol. 121, no. 2, pp. 1169–1186, 2021, doi: 10.1007/s11277-021-09055-1.
- [35] Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, 'A Survey on Zero Trust Architecture: Challenges and Future Trends', *Wireless communications and mobile computing*, vol. 2022, no. 1, 2022, doi: 10.1155/2022/6476274.
- [36] X. Wang, S. Mansour, and M. El-Said, 'Introducing Zero Trust in a Cybersecurity Course', New York, NY, USA: ACM, 2022, pp. 118–120. doi: 10.1145/3537674.3555779.
- [37] A. M. Abdelmagid, B. C. Ezell, and M. McShane, 'A Bayesian Network-Driven Zero Trust Model for Cyber Risk Quantification in Small-Medium Businesses', 2026, doi: 10.48550/arxiv.2601.06553.
- [38] L. Prates and R. Pereira, 'DevSecOps practices and tools', *International journal of information security*, vol. 24, no. 1, pp. 11-, 2025, doi: 10.1007/s10207-024-00914-z.
- [39] 'The problems with forcing regular password expiry | National Cyber Security Centre'. Accessed: May 19, 2026. [Online]. Available: <https://www.ncsc.gov.uk/blog-post/problems-forcing-regular-password-expiry>
- [40] 'The Orange Book Management of Risk – Principles and Concepts', GOV.UK. Accessed: May 21, 2026. [Online]. Available: <https://www.gov.uk/government/publications/orange-book/the-orange-book-management-of-risk-principles-and-concepts>
- [41] 'Regulation - 2022/2554 - EN - DORA - EUR-Lex'. Accessed: May 20, 2026. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng>
- [42] 'Cloud Security Posture Management: silver bullet or another piece in the cloud puzzle? | National Cyber Security Centre'. Accessed: May 26, 2026. [Online]. Available: <https://www.ncsc.gov.uk/blog-post/cspm-silver-bullet-or-another-piece-in-the-cloud-puzzle>
- [43] A. Johnson, K. Dempsey, R. Ross, S. Gupta, and D. Bailey, 'Guide for security-focused configuration management of information systems', National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-128, Oct. 2019. doi: 10.6028/NIST.SP.800-128.