

Final

by Jake Whitehouse

Submission date: 06-Jan-2026 04:24AM (UTC+0000)

Submission ID: 272229413

File name: 58181_Jake_Whitehouse_Final_712345_379464675.docx (68.11K)

Word count: 5176

Character count: 32024

GOVERNANCE OF AI AND MACHINE LEARNING SYSTEMS

Jake Whitehouse

Student University of Wales Trinity St David, Swansea, Wales

2406098@student.uwtsd.ac.uk

Abstract- AI and machine learning systems have brought advanced operational features to different business sectors, but they generate advanced security threats and ethical problems. The governance of AI and Machine learning systems needs to exist because it will protect against risks by maintaining regulatory compliance and upholding ethical standards for data management and model implementation. The research investigates methods that organisations can use to create AI governance systems which monitor potential risks and prevent unauthorised use and automatically identify problems and trigger automated responses. The discussion combines AI risk assessment with AI data and model ethical standards and compliance requirements and current AI governance systems and proposed methods for their optimal implementation. Organisations can establish trust in AI technologies while protecting against damage through their implementation of risk management systems and their commitment to ethical oversight and regulatory compliance during the AI development process.

I. Introduction

Artificial intelligence and machine learning operate as core business elements which help organisations boost operational performance and technological advancement. The deployment of AI systems creates positive results but simultaneously produces negative effects which impact risk management operations and ethical standards and regulatory requirements. Organisations that do not establish proper control systems will face social and financial damage because high-profile mistakes have shown AI systems can cause such problems. The online chatbot produced hate speech after someone manipulated it which showed that AI systems without supervision will create unpredictable harmful content that violates laws and harms public trust. AI systems

lack proper controls which has resulted in major social and ethical damage that demonstrates the need for governance systems to manage complex AI-related security threats. AI governance creates rules which protect society from technological advancement through security systems [1].

Organisations operating in the present day need to establish a system which predicts AI-related security threats and defends against established risks and identifies unauthorised activities and triggers immediate automated responses for detected incidents. A strong AI governance program needs to exist for this purpose. AI governance consists of established procedures and regulatory frameworks which maintain AI systems operate with safety and fairness and maintain accountability. Organisations can achieve effective governance through the implementation of oversight systems which defend against bias and privacy violations and misuse while they support technological development and build public trust. The system implements a controlled method to reduce possible negative effects through its implementation of AI ethics committees and data governance policies and model monitoring systems which stop flawed or harmful decisions from occurring [1].

The governing elements which control AI need additional study because their power base continues to expand. Organisations must now handle increasing regulatory

demands which include data privacy and algorithmic fairness standards that extend from GDPR to new AI-focused regulations which demand organisations to handle compliance as a fundamental requirement. Organisations operating in the present day must meet rising ethical expectations from their customers and public stakeholders because they need to minimize bias while making their AI decision systems transparent. Third the current situation reveals all possible adverse effects of AI because research shows that enterprises face three main obstacles to adopt AI technology which include explainability problems and bias issues and trust-related challenges. Business leaders identify AI ethics and trust issues as their main obstacle to implement sophisticated AI systems because 80% of them express such concerns [1]. The absence of suitable AI risk management systems creates obstacles which block technological progress.

The following sections of this paper will analyse (1) AI/ML system risk profiles and the necessity for modifying current risk management systems and (2) ethical standards which direct proper AI implementation and (3) AI governance systems and their corresponding regulatory frameworks and (4) methods to implement AI governance systems which protect against security threats.

II. Risk in AI and ML

Organisations need to prepare for risks which AI and ML systems introduce to their operational activities. The AI lifecycle contains technical risks which represent a major category of risks. The system faces three main types of problems which include data quality issues and model inaccuracies and security vulnerabilities. AI models receive discriminatory information through biased or low-quality training data which results in unfair and incorrect system

responses. An ML model would show unwanted behaviour and fail to correctly generalise data when it lacks proper control mechanisms which becomes a major issue for safety-dependent systems. AI systems become more vulnerable to adversarial attacks which target their operations. Attackers can use two methods to exploit ML models using malicious input data (adversarial examples) and training data contamination (data poisoning) to achieve model output manipulation. The Microsoft Tay chatbot became a well-known example when trolls exploited the system to create harmful content during its first week of operation [4]. The incidents demonstrate that threat actors use methods which standard IT security systems fail to protect against AI models thus needing developers to create defensive systems against these attacks.

The operational and oversight risks form their own distinct risk category. AI systems function independently to produce vital decisions which leads to increasing system failures at a rapid pace. AI decision errors would remain undetected until they produce major harm because there are no proper monitoring systems in place. The performance and fairness of models will deteriorate when data changes because models tend to drift during time periods without proper monitoring and update procedures. An AI system which starts as reliable will develop unpredictable behaviour and biased responses when no one monitors its operation. Organisations face two major risks from model drift because it leads to deteriorating product quality and compromised regulatory compliance. The organisation stays unaware of when their outputs start to violate established standards.

The system contains two risk categories because it encounters both ethical problems

and system infrastructure failures. Users cannot understand the decision-making process of AI because of its black box nature which creates problems when they need to explain results to people who have been impacted. The system faces two major problems because it lacks proper information which results in unfair decisions and discriminatory choices that simultaneously damage public trust in the system. The system faces two main obstacles which stem from maintaining accountability for dangerous AI choices that create uncertainty about developer or user responsibility and from algorithmic operations. The lack of defined terms for AI behaviour roles and accountability creates conditions which result in governance system failures.

The summary shows that AI/ML systems present four main risks which include system failures and human errors and discriminatory outcomes and system vulnerabilities and unclear operational processes. The system needs to identify these factors when designers create the system and when operators use it in their daily work. Organisations need to conduct complete risk assessments for AI applications which must evaluate data integrity and model robustness and cybersecurity and social effects of AI systems. The detection of system weaknesses becomes possible through stress-testing models which check for bias and through simulated adversarial attack simulations. Organisations need to understand their risk environment because this knowledge enables them to establish effective governance which helps them predict potential threats and create defensive measures.

III. Ethics and compliance

AI governance needs to handle both technical problems and it must protect

ethical standards and follow all applicable laws. The ethics community supports five core principles which direct responsible AI development through fairness and transparency and accountability and privacy and reliability. Organisations need to actively work against AI system discrimination through purposeful actions which prevent discriminatory results. Organisations need to choose training data which should have balanced content for this process while they must conduct algorithm audits to detect discriminatory patterns against various groups. Transparency means providing explanations for AI decisions and being open about when and how AI is used. The system needs to define specific roles which will handle AI system results and monitor all AI projects through the creation of AI ethics committees that bring together members from different organisational areas.

Organisations that want to use AI need to follow multiple new rules which continue to expand in number. The EU General Data Protection Regulation (GDPR) together with other data protection laws affect AI systems which process personal information because these laws establish rules for obtaining consent and protecting privacy and they sometimes demand algorithmic transparency. The GDPR framework contains regulations about automated decision systems and data management which determine the operational methods of AI systems. The implementation of sector-specific regulations exists because healthcare and financial institutions need to follow rules which govern model validation and risk management for their decision-support systems.

The EU's proposed AI Act along with other new AI regulations will establish mandatory requirements for high-risk AI

systems which need to implement detailed risk management systems and provide complete system visibility. AI governance stands as a vital priority which worldwide regulators must address because they need to create new regulations because there are no existing AI laws. The U.S. National Institute of Standards and Technology (NIST) published an AI Risk Management Framework (RMF) which serves as a guide for organisations to handle AI-related security threats [2]. The NIST AI RMF which appeared in 2023 offers organisations a voluntary framework to establish trustworthiness in AI systems through its measure and manage and govern functions.

Industry standards also contribute to compliance and best practices. The international standard ISO/IEC 38507:2022 establishes governance principles that organisations need to follow when they want to use artificial intelligence (AI) systems. The organisation helps corporate boards and leadership teams to use AI systems through transparent responsible methods which require suitable monitoring systems [3]. Organisations can prove their AI governance due diligence by implementing these established standards. The OECD AI Principles which more than 40 nations have accepted for developing trustworthy AI systems serve as an ethical framework that organisations can use to create their own policies before legal requirements become effective.

The AI development process needs legal and ethical checkpoints to be integrated at every stage to achieve compliance. The organisation needs to perform ethical impact assessments for AI system deployment and must track data origins and processing steps to protect privacy and maintain data quality and establish approval procedures which need risk assessment and

compliance verification from relevant teams. Regular audits of AI outcomes for bias or errors are also important to meet both ethical commitments and regulatory expectations. Governance functions as an ongoing process which needs permanent tracking and system adjustments because new regulations appear and AI technology undergoes periodic modifications and learning processes.

IV. Frameworks and best practices

Organisations need to create a structured AI governance framework which will enable them to manage AI-related risks and ethical concerns and stay compliant with regulations. Such a framework provides an organisational process for overseeing AI from conception to deployment and beyond. The essential components of a plan include policy guidelines together with defined roles and responsibilities and risk management processes and monitoring and response systems.

Organisations need to develop AI governance policies which will function as their organisational base. The organisation needs to establish its AI usage responsibilities through these established policies. The policy contains guidelines which ban AI systems that create dangerous or immoral situations or require human understanding for their AI systems which interact with customers. The policies receive their direction from top management which establishes that AI development teams need to make governance part of their operational processes. Multiple major organisations have implemented their AI governance systems through the current corporate governance frameworks which they use. An effective governance framework also defines roles and accountability. The organisation needs to create a Chief AI Ethics Officer position which should also

handle AI risk management duties under the Chief Risk Officer. The review and approval process for important AI implementations should involve cross-functional committees which include data science experts together with compliance specialists and IT security professionals and legal experts and HR specialists. The framework needs to establish methods for risk evaluation and protection strategies: The oversight committee needs to review results from bias testing and security testing and impact analysis which teams must perform on each AI project before deployment. Organisations need to implement AI governance through their current enterprise risk management systems according to best practices. The NIST AI RMF and similar guidelines encourage aligning AI risk controls with general risk management and cybersecurity framework [2]. Organisations should implement the NIST Cybersecurity Framework (CSF) for their AI assets in addition to their current framework. The NIST CSF 2.0 (2024) established "Govern" as a new function which combines policy administration with executive responsibilities and risk management planning and regulatory monitoring to support business goal achievement [5]. The current trend shows that organisations now understand governance as an independent security and risk framework which controls all security operations while connecting them to organisational objectives.

Continuous monitoring and incident response are vital components of AI governance. Organisations need to create monitoring systems which track AI system operational performance and behavioural patterns when staff members actively use these systems. Users can monitor three vital model performance indicators through dashboards which show accuracy metrics and fairness metrics by analysing

demographic error rates and detecting drift. The system features automated alert functionality which identifies when models operate outside their predefined operational boundaries. The system must execute its pre-programmed response sequence whenever it generates these particular alert messages. The organisation needs to stop the AI system operation while they use previous model versions and human reviewers for decision-making until all problems get fixed. The organisation needs to create an AI incident playbook which will enable them to handle AI model data breaches and evidence of bias that results in harm to people. The system runs automated responses which start when specific conditions happen because ML models for intrusion detection activate containment actions when they detect threats.

Organisations need to develop workplaces which support ethical awareness through AI training programs. The training of technical teams needs to concentrate on two essential areas which include understanding AI societal impacts and developing methods to establish ethical principles for their professional activities. Business stakeholders need to understand both the operational advantages and operational limitations of AI systems to develop suitable and equitable regulatory systems. Organisations need to establish governance systems for AI which enable staff members to review AI output and alert their superiors about any system problems they discover.

The governance of AI systems becomes more robust through scheduled auditing procedures and external validation methods. AI systems undergo evaluation through independent audits which combine internal assessments with third-party evaluations to confirm their compliance with established policies and regulatory requirements. The auditing process would

conduct privacy and bias assessments on datasets while it checks for both algorithm transparency and complete documentation requirements. Organisations need to join certification programs which assess their operational performance through ISO standards and government regulations to prove their commitment to industry-leading methods.

V. Conclusion

AI and machine learning technologies offer numerous advantages, but organisations need to actively govern their operational risks which exist by default. Organisations need to create full frameworks which link risk management to ethical standards and compliance rules to develop trustworthy AI systems which function effectively. AI/ML system governance allows businesses to detect potential threats before they occur while protecting their systems from both biased operations and unauthorised use and enabling them to identify system issues at their onset and trigger automated responses during security incidents. The evolving landscape of AI regulation and public scrutiny makes this governance imperative. Organizations which implement AI governance successfully will decrease their risk exposure while their AI projects will become safe and ethical and socially responsible through innovation.



Zero-Trust-Aligned Security Programme for ResilientIntellect Ltd

The company ResilientIntellect Ltd operates as a threat intelligence and consultancy firm which develops its own AI-based threat analysis software while its employees work between home and office environments. The company needs to follow DORA and NIS2 Directive regulations when it enters the EU market. We propose a Zero Trust-aligned security programme for the new EU unit to enhance cybersecurity and meet these obligations. Zero Trust operates on a “never trust, always verify” principle, meaning no user or device is trusted by default even if already inside the network [6]. The system performs continuous authentication and authorisation of all access requests through least privilege access, and it uses network segmentation to restrict attacker movement between segments [6].

A. Organisational Structure and Roles

The security team needs to create two essential positions which will lead this program: Cloud Security Architect and DevSecOps Lead. The Cloud Security Architect will create security protocols for cloud infrastructure and services which follow Zero Trust principles through proper identity management and access control and cloud network segmentation. The company maintains its wide cloud infrastructure deployment for storing data and operating AI models and other applications. is properly secured and

continuously monitored. The DevSecOps Lead will implement security practices throughout software and AI model development by performing vulnerability assessments on code and dependencies and AI models during the development process. The security of ResilientIntellect cloud operations and software supply chain will improve through the establishment of specialised experts who handle these specific domains. The CISO oversees these positions which work together with IT and develop

B. Policies and Procedures

Multiple updated policies need to exist which will direct users together with technical personnel through a Zero Trust security framework.

The organisation needs to develop an AI Usage Policy which will establish correct procedures for AI system operation and data management to protect security and maintain ethical standards. The system needs to perform bias testing on AI models while blocking production customer data usage for model training except when the data undergoes proper anonymisation and when human oversight exists for essential AI decisions. The policy defines rules for AI development at ResilientIntellect which supports ethical AI practices and follows all applicable data protection laws.

The system requires organisations to establish minimum security standards which must be applied to all SaaS applications and cloud services. The organisation needs to activate MFA authentication for all user accounts and SaaS applications should only receive necessary permissions. Security

configuration assessments need to run regularly to verify cloud storage bucket permissions and protect default credentials and APIs. All new third-party services need to undergo security risk assessments before organisations can implement them while their contracts need to include cybersecurity requirements. The policy enables DORA to fulfil its mission by overseeing third-party risk management operations.

The organisation needs to establish BYOD and Remote Work Policy which will specify security protocols which employees must follow when working from outside the office. All personal devices which access corporate resources need to run with current endpoint protection and device encryption and must establish their connection through secure pathways (e.g. corporate VPN or ZTNA client).

These policies create security limits which users and systems need to adhere to for correct system functioning. The implementation of these tools establishes a Zero Trust environment through their ability to eliminate all forms of automatic trust which requires every device and user and application to fulfil security requirements before obtaining access to resources. The evidence shows that the organisation takes active measures to handle risks which auditors must verify according to DORA/NIS2 standards.

C. Compliance with DORA and NIS2

Our programme explicitly addresses the requirements of DORA and NIS2. DORA is an EU regulation to ensure operational

resilience in the financial sector, emphasising comprehensive ICT risk management, incident reporting, and oversight of third-party ICT providers. The EU directive NIS2 establishes cybersecurity standards which apply to essential industries through its requirement for executive-level accountability and its emphasis on risk management and immediate incident disclosure [5]. The main compliance requirements consist of.

Senior leadership members will actively participate in cybersecurity governance activities under the Management Accountability system. The steering committee along with the board will perform security policy reviews to get approval while they maintain their ongoing practice of reporting cyber threats and their associated solutions. Both DORA and NIS2 mandate that top management be accountable for cybersecurity integration into business strategy [5], which this step fulfils.

The organisation needs to create a full ICT risk management framework which detects risks before starting their assessment process to create strategies for risk reduction. The organisation needs to make supply chain and third-party risk management its top priority because these elements fulfil essential requirements which both regulatory frameworks [5] demand. The program will keep track of security risks through a risk register which will also perform security background checks on all vendors. The program will verify that all essential service providers maintain solid security systems and business continuity protocols.

The system requires established procedures to detect incidents which staff members

need to report right away while they must respond with immediate action. Organisations under NIS2 law must alert authorities about significant security breaches which they need to report within a 72-hour period. The incident response plan will establish communication systems which will enable the organisation to notify regulators and affected clients about major cyber incidents that include data breaches and system outages within established time limits.

The organisation should perform Operational Resilience Testing which includes annual penetration tests and cyber crisis exercises to check security controls and response preparedness. Organisations need to conduct threat-based penetration testing on their critical systems according to the DORA framework. The team will conduct attack simulations to confirm both AI system and cloud infrastructure security against cyber threats and to detect system weaknesses which need correction. Regular testing and improvement will satisfy DORA's resilience testing requirements and NIS2's emphasis on preparedness.

The security measures at ResilientIntellect will fulfil both DORA and NIS2 core compliance requirements while providing enhanced security protection to the organisation. The organisation will prove to regulators that it has created cybersecurity governance which uses vendor risk assessment and incident response capabilities to manage risks systematically while meeting EU regulatory requirements.

D. Governance and Security Strategy

The NIST Cybersecurity Framework (CSF) 2.0 will serve as our security program framework because it provides a complete business-oriented solution. The NIST CSF 2.0 framework establishes a new "Govern" function which supports the security functions of Identify and Protect and Detect and Respond and Recover by making sure they serve organisational goals [8]. Our leadership team will determine security priorities and performance indicators which will guide security activities through ongoing assessment of their operational success and business value.

We map our security controls and processes to the five CSF core functions to cover all aspects of defence. Asset inventory and data classification systems help organisations achieve Identify while protective technologies such as firewalls and MFA and encryption serve to Protect. The combination of continuous monitoring systems with alert functions enables organizations to Detect security threats. Organisations should establish incident response plans to handle security incidents while maintaining backup systems for data recovery purposes. The Governance function serves as the highest level which enables management to monitor all policies and risk appetite and compliance requirements. The structured framework we adopt establishes defined responsibilities which protect all cybersecurity elements from being ignored. It also complements DORA/NIS2, since those regulations call for governance and risk management very much in line with CSF principles [5].

E. Risk Management Focus: Supply Chain and Cloud

The high-level risk assessment shows that software supply chain threats together with cloud system configuration vulnerabilities create the most severe risks for ResilientIntellect's new business entity. Our development pipeline will receive enhanced security measures which will protect our software supply chain from risks that stem from using compromised open-source libraries and poisoned AI models. The system will perform automated dependency scanner checks on all open-source dependencies to detect known vulnerabilities. The system will verify all external code and models through checksum verification and retrieval from authorised repositories. The developer training program will teach participants to track third-party components and phishing attacks because these threats could bring security vulnerabilities through the insertion of harmful code. The system monitors supply chain attack alerts through threat intelligence to activate security responses which include security patch

deployment and elimination of vulnerable system elements.

For cloud risks, we use a Cloud Security Posture Management (CSPM) tool to continuously audit our Azure/AWS configurations for misconfigurations or policy violations. The Cloud Security Architect will implement best practices through his work which includes protecting cloud storage buckets from unauthorised access and implementing MFA protection for administrative interfaces and secure storage of cloud API keys. We apply least privilege to cloud identities and segment cloud networks so that even if an attacker compromises one cloud resource, they cannot freely access others.

F. Contingency Planning: Ransomware Scenario

Our programme maintains operational resilience through a comprehensive disaster recovery (DR) plan which protects against the most severe possible situations. A ransomware attack which encrypts our AI training data and source code repositories represents one such situation. Our contingency measures for this include:



Figure 1: High-Level Zero Trust access model for ResilientIntellect Ltd, enforcing continuous verification and least-privilege access.

The system performs scheduled backup operations which store essential data including source code and model training information and client information in protected storage that operates independently from the main network. "The term "immutable" protects backups because it makes them inaccessible to modification or deletion during their defined retention duration which blocks attackers from removing backup data. The system operates

with multiple backup systems which we store at locations separate from the main site. The system preserves clean data copies which protect production data from ransom attacks when they occur.

Incident Response and Recovery: The incident response plan contains procedures which enable organisations to stop ransomware attacks through system isolation during the first response phase, and it activates the response team and enables backup system operation when available. The organisation uses backup data instead of giving in to ransom demands. The system requires a complete rebuild after malware removal because the team needs to restore data from backup files which were created at the most recent point. The process planning will enable us to reduce the duration of operational interruptions. If our AI model training environment is encrypted, for example, we can rebuild a fresh environment and load recent training data to resume operations quickly.

The organisation will develop backup operational systems for vital operations which will enable business operations to continue. The team can access vital work through read-only mirror access or local git clones when the main code repository becomes unavailable until the system returns to operation. The system will start a backup cloud instance for client-oriented services when the main instance becomes unavailable to prevent service disruptions.

The DR plan includes communication templates which help us alert customers and regulators about incidents and our recovery status when necessary. Organisations need

to maintain absolute transparency to protect public trust during major emergency situations. We will communicate promptly and factually after containing the situation, demonstrating control and continuity of service.

Through these contingency plans, ResilientIntellect can withstand a ransomware attack (or other major cyber incident) with minimal lasting damage. The organisation will maintain operational readiness for effective response and recovery through scheduled drills and DR plan updates which regulators and frameworks require for operational resilience.

G. Key Protection Mechanisms

The program will implement modern security controls which support Zero Trust principles to fulfil all necessary requirements from the scenario.

Phishing-Resistant MFA: The system will require all users to authenticate their logins through multi-factor authentication which uses FIDO2 security keys and app-based push authentication as its phishing-resistant authentication methods. The security measure implementation protects users from credential theft attacks because attackers must possess both password information and an additional authentication factor to gain system access. Strong MFA is increasingly seen as a baseline requirement for cybersecurity and is explicitly encouraged by regulators and cyber insurers [7].

The system will use Zero Trust Network Access instead of its current wide VPN access system. Users access internal applications through ZTNA which provides a protected broker that checks their authentication status and device security level and session requirements for each connection attempt. The system provides network access to authorised services but blocks all other network resources. The system restricts attackers from moving laterally because they cannot access internal systems even when they gain control of an account. The ZTNA portal demands remote developers to authenticate before they can access the code repository and its associated services following their completion of all security verification requirements. Everything else remains off-limits.

The system will obtain sophisticated EDR software which will track servers and laptops for detecting any indications of unauthorised behaviour. The EDR system will activate network isolation for endpoints which show malware or anomalous activities such as process-based file encryption at high speed which ransomware operations would perform.

The system will combine cloud posture monitoring with SIEM and CSPM functions to identify security threats when they first appear. The CSPM tool runs automated assessments of our cloud infrastructure on a continuous basis to identify security misconfigurations and compliance violations which produce alerts when firewalls show open ports or when new cloud resources emerge without appropriate security groups. In parallel, a Security Information and Event Management (SIEM) system will aggregate logs from

across the organisation – firewall logs, authentication logs, application logs, etc.

The security controls at ResilientIntellect establish multiple protection layers which operate under Zero Trust principles. The implementation of MFA with ZTNA provides enhanced security for identity and access management systems through least privilege access and network segmentation which limits attack paths from compromised systems. The security system uses EDR together with SIEM/CSPM to detect and respond to breaches at high speed. The security measures we implemented have proven effective in defending systems against real-world attacks while we follow present-day security standards to minimise attack impact and preserve business activities.

Conclusion

The Zero Trust-aligned security programme which we propose will provide ResilientIntellect Ltd with an advanced protection system which will defend the company during its EU market entry. The organisation implements security roles which establish specific boundaries to manage AI operations and SaaS management and Bring Your Own Device access for achieving operational compliance with DORA and NIS2 standards. The NIST CSF-based governance model provides continuous assessment and improvement of security efforts through management oversight. The organisation has established risk management protocols which defend against supply chain threats and cloud-based attacks, and it maintains operational readiness through established contingency

plans for predicting and surviving non-critical incidents. The implementation of modern security controls which include phishing-resistant MFA and ZTNA and EDR and CSPM/SIEM creates multiple protection layers that provide complete visibility to users.

REFERENCES

- [1] IBM, “What is AI governance?” IBM Think Blog, 2023.
- [2] National Institute of Standards and Technology, **AI Risk Management Framework 1.0**, Jan. 2023.
- [3] **ISO/IEC 38507:2022**, *Information technology – Governance of IT – Governance implications of the use of artificial intelligence by organizations*, ISO, 2022.
- [4] V. Fordham, A. Diehl, and D. Caswell, “Securing government against adversarial AI,” *Deloitte Insights*, 2022.
- [5] A. Jamil, “DORA and NIS2: Connection Points and Key Differences,” *ISACA Now Blog*, June 5, 2025.
- [6] NIST, **Zero Trust Architecture**, Special Publication 800-207, Aug. 2020.
- [7] L. Trosciancki and E. Weijdema, “2025 Compliance: DORA, NIS2, CRA Reporting Explained,” *Veeam Blog*, Feb. 2024.
- [8] D. Bonderud, “Unpacking the NIST Cybersecurity Framework 2.0,” IBM Blog, Mar. 2024.

Final

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

67 /100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

JAKE WHITEHOUSE

67

ENGAGEMENT WITH LITERATURE

All work must be appropriately researched and referenced with an extensive range of relevant and credible literature. High-level referencing skills consistently applied. Most references should be current and Laws must cite current legislation in the appropriate government site(s). (20 marks)



The work engages with relevant sources, though the use of academic literature is limited and there is some reliance on general web-based material. Referencing is present throughout.

14

KNOWLEDGE AND UNDERSTANDING

You will need to show application of skills and research in the assignment by demonstrating critical understanding of the well-established concepts and principles of the subject and the main methods of enquiry. May go beyond established theories.(10 marks)



The submission shows adequate understanding of key security and governance concepts, though explanations are often basic and not always fully developed.

8

COGNITIVE AND INTELLECTUAL

Marks will be awarded: For critical analysis and evaluation, based on the quality of the documentation/report/paper. How relevant conclusions are drawn and justified. (25 marks)



There are critical evaluation, with the work tending towards description of established practices. Arguments would benefit from more explicit justification and engagement with evidence.

18

PRACTICAL SKILLS

Marks will be awarded based on the quality of and level of detail provided for the design approach; diagrams, tables, charts and any other design methods utilise will enhance marks. These should be properly explained and contextualised. (25 marks)



Only a Zero Trust diagram provided. No organisation chart or table. More diagrams could be included..

Note, marks will be awarded based on the quality of and level of detail provided for the design approach; diagrams, tables, charts and any other design methods utilise will enhance marks.

10

TRANSFERABLE SKILLS FOR LIFE

This will be assessed based on the written and presentational quality of your report: • Flow • Professionalism • Comprehension (grammar and spelling) • Completeness and presentation of report (20 marks)



The report is generally readable and logically organised. Professionally done; formatting and

17

presentation.