

Assignment

by Dylan Hocking

Submission date: 10-Jan-2026 07:17PM (UTC+0000)

Submission ID: 272765102

File name: 50845_Dylan_Hocking_Assignment_712345_1792250956.docx (440.2K)

Word count: 2295

Character count: 12397



RESEARCH AND CASE SCENARIO

Data Security and Compliance (ACCA5034)

Dylan Hocking (2312757)
2312757@student.uwtsd.ac.uk

Table of Contents

1. Task 1	2
1.1. Introduction.....	2
1.2. Securing the Hybrid Workforce ..	2
1.3. Zero Trust Network Access.....	2
1.4. Secure Access Service Edge	2
1.5. Data Loss Prevention	2
2. Task 2	3
2.1. Introduction.....	3
2.2. Structure Design	3
2.3. Policies and Procedures	3
2.4. Compliance	3
2.5. Governance and Strategy	4
2.6. Risk Management.....	4
2.7. Contingency Planning.....	5
2.8. Protection Mechanisms.....	5
3. Conclusion	6
References	6

1. Task 1

1.1. Introduction

In this task the author was tasked to research and write a paper on a topic, the author chose the topic of securing the hybrid workforce. A hybrid workforce model combines the ability to work in the office or do remote work this is done through the cloud. This model works for employees where their work is mostly computer based [1].

1.2. Securing the Hybrid Workforce

Securing the hybrid workforce is very important as employees that work from home will need access to the company network because they might use personal devices or public networks [2]. Many companies do not realize the importance of securing the hybrid workforce and they underestimate cyber threats [3].

The best way of securing the hybrid workforce is by multiple levelled security put in place. One way is having a multi-factor authentication, this makes it so the users must give two or more ways to enter the system like a password and a code sent to their phone. But the most important way is training the employees to know how to spot phishing attacks and how to keep passwords secure [2][3]. There are many more ways of securing the hybrid workforce which will be talked about in the next few paragraphs.

1.3. Zero Trust Network Access

The Zero Trust Network Access (ZTNA) is a way to put in place a zero-trust security model, this will help protect from risks from both inside and outside the companies' network. This works by making one to one connections between the users and what

they need access to. For the user to create this connection they need to go through verification of themselves and their devices, this connection will need to be re-verified occasionally. ZTNA hides IP addresses from the network, the user's device can only see the IP addresses of services that it is using. It also checks if the device is trusted or not. The system also checks the repetitiveness of the requests to log on and how often this happens. ZTNA is built on the Internet while using encrypted Internet connections for the user and services that they are using [4]. ZTNA is a very useful tool to help secure a hybrid workforce as this helps verify employees' identities, this will help protect the network and protect them outside of the network as well.

1.4. Secure Access Service Edge

Secure Access Service Edge (SASE) is a cloud-based method on connecting users and their devices to a central cloud-based service instead of the private network of the organization. Some of the advantages of this are that new services can be added to the cloud-based service a lot quicker. SASE is also easier and cheaper for a company to manage. This cloud-based method is identity driven and not location driven, this means that an identity is placed on every user, service or device in the company. What that allows for is that the identity will follow the user or device to wherever they need the services. SASE also can work with multi-factor authentication and data loss prevention rules can be added as well [5].

1.5. Data Loss Prevention

Data Loss Prevention (DLP) is a method of preventing unsafe use and sharing of important data. DLP is about systems and employees that work to detect and stop important data from being leaked.

There are four main things to understand, they are knowing your data, protecting your data, preventing data loss and governing your data. Doing this will have benefits like for instance it will be easier to monitor the systems, detect problems and then block the unsafe or suspicious activity on the company's system. Some of the best ways to help with DLP is by using behaviour analytics to understand the users on the system and how they use it [6]. This is very important as loss of data can cost the company a lot of money and reputation as customer will not trust a company that loses their data, especially if that data is sensitive. Customers could also sue the company for these reasons.

2. Task 2

2.1. Introduction

The author is tasked with designing a Zero-Trust-aligned security programme for a company called ResilientIntellect LTD. Which is a company that does consultancies and creates its own AI threat analysis software. They use a full hybrid workforce. They give advice about which tools and frameworks to use for their customers, which their cloud storage and services is included.

2.2. Structure Design

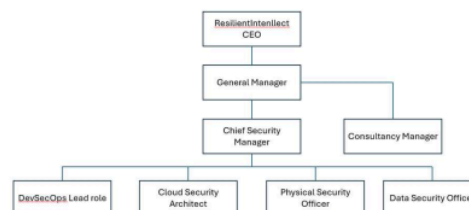


Figure of the author's design of an employee structure for the company ResilientIntellect LTD.

2.3. Policies and Procedures

Developing policies for AI usage in ResilientIntellect LTD. When making policies the author must make sure it is within laws and regulations. They also need to keep the policies up to date regularly as AI is evolving a lot in recent years. One of the most important policies that can be created is an employee training policy, this will help employee understand the uses and risks of AI. The next policy is about protecting data so that any sensitive data is not given to the AI. The third policy is that employees must know what an acceptable use is and what is not. The reason why companies should have AI policies are because AI can automate lot of tasks that are repetitive but it does have risks which will hopefully be minimized with policies in place [7].

2.4. Compliance

Compliance with the Digital Operating Resilience Act (DORA) is important because as financial aspects are getting more reliant on technology it makes cyber security even more important. DORA covers Information and

Communications Technology (ICT) risk management and ICT related incidents. It also covers resilience testing for digital operations and covers sharing information [8].

The Network and Information Systems Directive 2 (NIS2) purpose is to get cyber security all over the European Union to the same level to help with the growing number of cyber-attacks. Some of the security measures that are needed are multi-factor authentication, the use of cryptography, encryption and risk assessments. The reason why NIS2 is important for this company is because as ResilientIntellect LTD are a third-party provider they need to make sure that they are defended from cyber-attacks as attacks could also affect customer's system if they are using ResilientIntellect LTD services [9].



Figure of NIS2 different cyber-security measures. [10]

2.5. Governance and Strategy

A governance model that is based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). One of main parts of the NIST CSF is that the leadership holds responsibility for accepting policies and assigning resources. The other main parts it also makes sure that at a

security risk is treated a risk to the business. As a third-party provider NIST CSF is important as it helps with reporting and helps teams work together as it is a shared system which will help with communications. One of NIST CSF best strengths is its flexibility it can scale depending on the size of the company and it works well with other frameworks [11].

2.6. Risk Management

NIST has an approach that is helpful for risk management which is Frame Assess Respond Monitor (FARM). Frame is where companies set themselves up with different limitations, risk threshold and priorities for risk management. Assess is when the company assesses if there are any risks that are over the threshold or not on their systems and if they will result in loss or damage to their systems or data. If the risk assessment has found risks that are over the threshold this approach will move to the next stage being Respond. This stage is about what course of action is best for the risks and then implement those changes to lower the risks below the threshold. Monitor is about monitoring the third-party service that ResilientIntellect LTD providers and then continue or change the risk threshold appropriately. This can affect the company but they should make a plan so that this does not happen. Before they do anything, they might need to contact any type of supplier that would be affected [12, pp. 6-7].

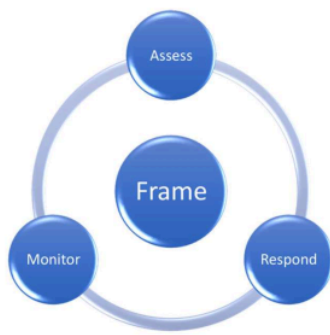


Figure of the NIST approach FARM.

[12, p. 6]

2.7. Contingency Planning

A Contingency plan is a plan that if things go wrong, like a natural disaster or the company's computer system gets effected by virus or malware. A plan should have to be in place so that the company can get back in operations as soon as possible. The advantage of having a contingency plan is that it helps to keep the risks and the actions that will lower the risk in mind. A contingency plan will also help with having a plan on what to do if something goes wrong so they can use the plan as soon as possible. A contingency plan will have to be constantly looked at and updated on a regular basis[13].

One of the reasons why contingency plans are important is because of things like ransomware. Why it's so important to have a contingency plan for ransomware is because it is a type of malware that stops the user from accessing the computer or the data on it. Then the hacker will contact them to pay them a sum amount of money for them to unlock the computer or data.

The hackers most of the time will not unlock the data or computer and if the user does not pay they will threaten to release the data to the public [14].

First thing that the company ResilientIntellect LTD needs to do is to make a contingency plan and to know what their most important assets are. The company also need to know how much they would be affected if they were locked out by ransomware. The company must keep multiple up to date backups which should all be stored in different places, for instance, the cloud, a hard copy which is kept off site and a backup server that is disconnected to the rest of the systems to keep it from being infected as well. The last thing they might need to do if they are attacked is that they need to look back on the attack and see where the problem was and how to fix it. They then need to write a report of the incident so the same thing cannot happen again [14].

2.8. Protection Mechanisms

For the company ResilientIntellect LTD the author would suggest that they use Cloud Security Posture Management (CSPM) this is because ResilientIntellect LTD does have cloud services which employees and customers can use. CSPM is a way to automate monitoring the cloud service and looking for threats. The reason why the author suggests using CSPM is because of the advantages that it brings. The first advantage is that CSPM is automatically checking the cloud

services throughout the day and night. It can give helpful information on how to improve the security, it also will update automatically with the changes with compliance [15].

3. Conclusion

The author in this report has done research on securing the hybrid workforce using ZTNA, SASE and DLP. They then needed to design and justify security for a company called ResilientIntellect LTD. The author needed to design an employee structure and write policies for the company. They also needed to write about compliance with DORA and NIS2. The next thing they needed to do was to design a governance model that was based on NIST CSF. The author then needed to write about risk management and then create a contingency plan. Then finally suggest protection mechanisms for the company the author suggested CSPM.

References

- [1] "Hybrid Workplace: The Future of Work." Accessed: Nov 21 2025. [Online]. Available: <https://www.sap.com/products/hcm/what-is-a-hybrid-workplace-model.html>
- [2] S. Gagi."Hybrid Workforce Security: Best Practices" *Labyrinth Technology*. (-09-252024). Accessed: Nov 28, 20252025, [Blog]. Available at: <https://www.labyrinthit.com/hybrid-workforce-security-best-practices/>
- [3] "Device Security in a Hybrid Workforce | Samsung Knox Blog." Accessed: Nov 28 2025. [Online]. Available: <https://www.samsungknox.com/en/blog/managing-device-security-for-a-hybrid-workforce>
- [4] "What is Zero Trust Network Access (ZTNA)?" Accessed: Dec 20 2025. [Online]. Available: <https://www.cloudflare.com/learning/access-management/what-is-ztna/>
- [5] Z. Kerravala, "How SD-WAN is evolving into Secure Access Service Edge: Secure access service edge (SASE), pronounced 'sassy,' combines elements of SD-WAN and network security into a single cloud-based service. It supports all types of edges, including WAN, mobile, cloud, and edge computing," 2019,
- [6] "What is data loss prevention (DLP)? | Microsoft Security." Accessed: Jan 5 2026. [Online]. Available: <https://www.microsoft.com/en-gb/security/business/security-101/what-is-data-loss-prevention-dlp>
- [7] "Building Effective AI Policies in the Workplace." Accessed: Jan 5 2026. [Online]. Available: <https://sytech-consultants.com/building->

[effective-ai-policies-in-the-workplace/](#)

[dfe4-48f2-97ec-6aa3b6c40cc4/content.](#)

[8] "Digital Operational Resilience Act (DORA) - European Insurance and Occupational Pensions Authority." Accessed: Jan 5 2026. [Online]. Available: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

[9] "What Is NIS2? | Compliance and Policies." Accessed: Jan 6 2026. [Online]. Available: <https://www.akamai.com/glossary/what-is-nis2>

[10] "NIS-2 : The impact of the Network and Information Security Directive on cyber security in Europe" *IN Groupe*. Accessed: Jan 6, 2026, [Blog]. Available at: <https://ingroupe.com/insights/nis-2-what-impact-for-companies-organizations-cyber-security-europe/>

[11] "NIST Security Governance Model for Modern Organisations" (-01-032026). Accessed: Jan 6, 2026, [Blog]. Available at: <https://www.neumetric.com/journal/nist-security-governance-model-5161/>

[12] K. Onu, "Software Supply Chain Risk Management Framework," 2021, Accessed: Jan 7, 2026. Available at: <https://repository.gatech.edu/server/api/core/bitstreams/93f69f9a->

[13] "What is Contingency Planning and why is it important?" *Henderson Loggie*. (-08-012023). Accessed: Jan 10, 2026, [Blog]. Available at: <https://hlca.co.uk/resources/what-is-contingency-planning-and-why-is-it-important/>

[14] "Mitigating malware and ransomware attacks." Accessed: Jan 10 2026. [Online]. Available: <https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks>

[15] "What is CSPM? | Microsoft Security." Accessed: Jan 10 2026. [Online]. Available: <https://www.microsoft.com/en-gb/security/business/security-101/what-is-cspm>

Assignment

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

46/100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

GRADING FORM: L5 DSC (ACCA5034)

DYLAN HOCKING

46

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)



Engagement with literature is weak and largely non-academic. The majority of references are blogs, vendor sites, and explanatory web pages (e.g., Microsoft, Cloudflare, Akamai, Samsung, SAP). There is almost no peer-reviewed or scholarly literature, and very limited use of authoritative regulatory texts (e.g., EUR-Lex, ENISA). Sources are used to describe rather than analyse or compare, which significantly limits marks.

9

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)



Demonstrates basic understanding of ZTNA, SASE, DLP, NIST CSF, DORA and NIS2. However, explanations are simplistic, sometimes imprecise, and frequently read like paraphrased vendor guidance rather than academically grounded explanations. There is no evidence of deeper conceptual understanding.

6

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)



The work is almost entirely descriptive. Task 1 explains technologies; Task 2 explains what the company “should” do. There is little to no critical evaluation, trade-off analysis, or strategic reasoning.

For example:

- ZTNA, SASE and DLP are described but not compared or critiqued
- NIST CSF, DORA and NIS2 are summarised but not analysed in relation to the organisation
- Risk, governance and contingency are presented as lists of good practice, not as reasoned design choices.

9

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)



Visual evidence present:

- An organisation structure figure
- A NIS2 measures figure
- A NIST FARM model figure

However:

- Figures are not numbered or explained

12

properly/referred to in report discussion.

- There is no architecture diagram, no Zero-Trust flow, no risk table, no governance matrix; some of these could enhance this section.

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 poorly written and weakly presented. Issues include:

- A number of grammar and sentence-structure errors
- Paragraphs are not fully justified
- Very basic academic tone
-

Structure is present (sections, headings, references), but professionalism is low.

10