

Assignment1

by Dylan Kempton

Submission date: 20-Jan-2026 01:38PM (UTC+0000)

Submission ID: 273844285

File name: 58175_Dylan_Kempton_Assignment1_712345_801033922.docx (27.86K)

Word count: 1323

Character count: 7523

SECURITY AND COMPLIANCE ASSIGNMENT 1

Dylan Kempton 2411039

Contents

Task 1 – Research in Data Security and Compliance	1
Compliance in a Fragmented World .	1
Data audit	2
Update privacy notices	2
Implement data protection.....	2
Train employees	2
Establish a response plan for data breaches	2
Review and update data protection measures	2
Digital Operational Resilience Act.	3
NIS2 Directive.	3
Task 2 – Case Scenario	3
Compliance	4
Governance & Strategy.....	4
Risk Management	4
Contingency Planning	4
Bibliography	5

Task 1 – Research in Data Security and Compliance

Compliance in a Fragmented World:

For organisations to ensure GDPR compliance they need strategies that are practical and can be implemented to meet the standards of the GDPR.

Data audit

One such strategy is to conduct a data audit, which will allow the organisation to map out every bit of data that is being collected and then categorise the data. This will help the organisation to identify areas of potential risks to the personal data that is traveling between the organisation and outside the organisation.[1]

Update privacy notices

Another thing Organisations can do is updating the privacy notices to ensure that users understand the privacy notices and that the notices are clear, concise, and transparent. The notices should inform users of their rights regarding the GDPR and how the data they supplied will be used.

Implement data protection

Organisations can implement data protection to their new services or products when they are being designed and built so the organisation does not need to worry about forgetting to add protection to their services or products and letting users' data be compromised making the organisation lose user trust, be in breach of the GDPR and also make the organisation frantically try to implement the data protection which may not be up to standards or accidentally leave a vulnerability.

Train employees

Organisations should train employees regularly on the GDPR and data protection, however it should be mandatory for employees that are in a position where they manage and deal with personal data.

Establish a response plan for data breaches

Establishing a data breach response plan should be one of the first things an organisation does as it will include procedures for what to do and who to contact during the data breach, the plan will also include the organisations plan to detect and report breaches and then investigating how it could have happened and what was lost.

Review and update data protection measures

Organisations should review and update their data protection measures regularly as exploits and other vulnerabilities would appear so they must keep on top of everything that comes up so they are able to stay in compliance with the GDPR and for their data protection to be effective.

Digital Operational Resilience Act

The Digital Operational Resilience Act (DORA) is a regulation introduced by the European Union (EU) to strengthen the online safety of organisations handling money. It came into effect on 17 Jan 2025 and ensures that banks, insurance companies, investment firms, consultant companies and other companies can protect themselves against cyber threats or respond and recover in the event of a systems failure.[2]

NIS2 Directive.

The NIS2 Directive is a framework to uphold cybersecurity in 18 sectors across the EU. It also makes member states collaborate with the EU for cross-border reaction and enforcement. NIS2 raises the EU common level of cyber-security with clearer rules and stronger supervision tools. It also introduces new risk management measures and reporting requirements to organisations from more sectors and setting up rules for cooperation, information sharing, supervision, and enforcement of cybersecurity measures.[3]

Task 2 – Case Scenario

ResilientIntellect Ltd is a fast-growing threat intelligence and consultancy company that develops its own AI-powered threat analysis software and uses a fully hybrid workforce. It assists businesses to proactively combat real and immediate threats from cyber-attacks. ResilientIntellect also use their consultancy services to provide the right tools and frameworks solutions to their customers state of compliance, business continuity, data recovery and risk management which includes their cloud storages and services.

The company is expanding into the EU and must comply with DORA and NIS2. They require a Zero-Trust-aligned security programme for their new unit which must be designed and justified.

The new information security unit will need policies and procedures for AI usage, secure SaaS configuration and BOYD for hybrid workers. They will also need to address how they will meet DORA's requirements and NIS2 obligations. A governance model based on NIST 2.0 cybersecurity framework that links the security strategy to the goals

of the organisation. A high-level risk assessment focusing on software supply chain risks and cloud misconfigurations needs to be conducted. And a contingency plan needs to be thought up to plan for malicious cyber-attacks such as ransomware attacks.

Compliance

The European Supervisory Authority (ESA) should participate in policy discussions and the technical workings of the organisation and be able to exchange information and further cooperation between the organisation and the ESA. The organisation should also be able to request technical advice from the competent authorities designated or established in accordance with Directive 2022/2555 such as the ESA and establish cooperation arrangements that aim to ensure effective, coordinated and fast responses.[4]

To keep total control over any IT risks, the organisation needs to have an effective IT risk management, as well as policies for handling all IT related incidents and for reporting major IT related incidents. The organisation should have policies in place for testing IT systems, as well as for managing IT third-party risk. [4]

The relevant national supervisory arrangements in respect of the organisation should take into account the size, overall risk profile, and the nature, scale and complexity of their services, activities and operations even when the relevant thresholds established in Article 5 of Directive 2016/2341 of the European Parliament and of the Council (10) are exceeded. [4]

Governance & Strategy

Risk Management

Contingency Planning

In case of a ransomware attack there should be offsite backups which will back up daily by using the cloud, so in the event of a ransomware attack only the training data and source code from that day is lost and the organisation is able to back up the AI training data and the source code from the day before once all the systems are wiped clean of the ransomware.

When a ransomware attack happens, the affected device must be quarantined imminently to stop it spreading, then the malware must be removed and the weakness in the security needs to be analysed and improved to stop another breach from the

same weakness, also make sure to notify the local law enforcement about the breach. After the malware is removed, change all organisation passwords immediately. If system downtime will affect the customers, inform them about the breach though assure them that their data is secure and that security is being toughened and thank them for their patience and understanding, because it is better for the customers to find out from a leaked source then their trust will be damaged and they may go elsewhere.

Bibliography

- [1] P. Venkatraman, "How to navigate GDPR compliance challenges - Intuition," Intuition, Jun. 13, 2024. [Online]. Available: <https://www.intuition.com/how-to-navigate-gdpr-compliance-challenges/> [Accessed 29/12/25]
- [2] Eiopa, "Digital Operational Resilience Act (DORA)" Dec. 15, 2025. [Online]. Available: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en [Accessed 01/01/26]
- [3] European Commission, "NIS2 Directive: securing network and information systems" Jul. 1, 2025. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive> [Accessed 05/01/26]
- [4] European Commission, "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector" Dec. 14, 2022. [Online]. Available: <https://eur-lex.europa.eu/eli/dir/2022/2556/oj/eng> [Accessed 14/01/26]
- [5] European Commission, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)" Dec. 27, 2022. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555> [Accessed 14/01/26]

Assignment1

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

32/100

PAGE 1

QM

Cover page

Separate cover page

QM

New page

Start on new page

PAGE 2

PAGE 3

PAGE 4

PAGE 5

GRADING FORM: L5 DSC (ACCA5034)

DYLAN KEMPTON

32

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)



Your submission engages with a small range of relevant sources, primarily regulatory and practitioner-based. Academic depth and synthesis are limited, and referencing is basic.

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)



Your work demonstrates basic understanding of GDPR, DORA, NIS2, and security governance. Explanations are correct but high-level and brief, indicating limited conceptual development.

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 submission is predominantly descriptive, outlining required actions and controls with

8

minimal analysis or justification. There is little evidence of critical evaluation or strategic reasoning.

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)



There are no diagrams and no visual models. The work relies entirely on narrative description, with no architectural, organisational, or governance. Please see specific guidance in the assignment brief.

0

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 readable and logically ordered, but very brief, with limited academic depth, minimal formatting sophistication, and basic referencing. IEEE two-column format not use.

9