

Frist class

**ASSIGNMENT SERVICE**

that you deserve



# SAMPLE FOR ASSIGNMENT 70+DI

From Dr.Khanh Assignment Service

THÔNG TIN LIÊN HỆ:



DrKhanhAssignmentService



[www.drkhanh.edu.vn](http://www.drkhanh.edu.vn)



(+84) 939 070 595 hoặc (+84) 348 308 628

# One stop-solution for your academic stress



## Essay Writing



**Professional writers craft custom essays tailored to your specific requirements and academic standards.**

- ▶ Plagiarism-free guarantee
- ▶ Timely delivery
- ▶ Expert writers in diverse subjects

## Assignment Assistance



**Expertly crafted helps for all tasks.** Consultation services where experts provide guidance on understanding assignment requirements, brainstorming ideas, and structuring your work.

- ▶ Clarification of assignment instructions
- ▶ Brainstorming sessions
- ▶ Topic suggestions

## Dissertation & Thesis Help



**Specialized guidance for graduation and research projects.**

Comprehensive assistance for thesis and dissertation writing, from topic selection to final draft refinement.

- ▶ Access to scholarly sources
- ▶ Data analysis support
- ▶ Formatting adherence

## Proofreading & Editing



**Professional refinement of papers.**

- ▶ Grammar and spelling correction
- ▶ Style improvement
- ▶ Formatting assistance

## Online Tutoring Sessions



**Personalized support to boost understanding.**

One-on-one tutoring sessions conducted online to help students grasp difficult concepts and improve their grades.



- ▶ 24/7 availability
- ▶ Step-by-step explanations
- ▶ Experienced tutors
- ▶ Interactive whiteboard tools
- ▶ Flexible scheduling

## Exam Preparation



**Prompt aid for all subjects.**

Resources and guidance to help students prepare for exams, including study guides, practice tests, and exam-taking strategies.

- ▶ Subject-specific study materials
  - ▶ Mock exams
  - ▶ Time management tips
- 
- 

Assignment 1: Business Report

Course Code	<b>INTE2585</b>
Course Name	<b>Introduction to Cybersecurity Governance</b>

**TABLE OF CONTENTS**

- 1. Part 1: Risk and Compliance Assessment
  - 1.1 Company .....3
  - 1.2 Compliance Management .....4
  - 1.3 Risk Management.....4

2. Part 2: Cybersecurity Policy Development

Organizational Structure for Cybersecurity

1.1 Organizational Structure for Cybersecurity.....5

1.2 Role Alignment and Interactions .....6

Cybersecurity Policy

2.1 Policy Coverage and Relevance .....6

2.2 Policy Practicality and Enforceability .....7

2.3 Review and Revision Mechanism.....8

3. REFERENCES:.....9

**Declaration and Statement of Authorship**

This assignment is my original work and no part of it has been copied from any other student’s work or from any other source except where due acknowledgement is made.

## Part 1: Risk and Compliance Assessment

### 1.1 Asset Management

Healthcare asset management is essential to healthcare operations, as mandated by the standard ISO55000-Asset Management. Proper asset management provides better visibility into hardware, software, data, services, and people, reducing the risk of vulnerability to several threats (Volchkov 2018). An out-of-date system or relying on spreadsheets can create risks, and dedicated asset management systems can help healthcare organizations better respond to incidents, allocate resources efficiently, and comply with regulations.

With the evolution of cyber threats, CyberGuardian HealthTech can improve its cybersecurity posture and protect patient data by identifying and prioritizing essential assets and keeping track of developments. Strict access restrictions ensure that only authorized individuals can access confidential information. This includes user authentication methods like passwords, multi-factor authentication (MFA), and role-based access controls (RBAC) to restrict access to particular assets based on job duties and responsibilities (EDPB 2020).

Data protected by asset protection standards (ISO 27001/2) when at rest and in transit provides an additional safeguard against the unlawful disclosure of sensitive information. To reduce the possibility of data breaches, encryption techniques should be implemented to secure financial information, personnel records, and patient health records. Continuous monitoring by requiring regular supervision. Robust monitoring technology can detect suspicious or unauthorized access attempts in real-time. Continuous system and network monitoring enables companies to detect and repair security issues, minimizing their impact (Sikdar 2022).

### 1.2 Compliance Management

Key rules for CyberGuardian HealthTech must be identified and understood by thoroughly researching and understanding the healthcare industry's legal and regulatory standards. This method requires mapping, interpretation, and investigation (Koop & Lodge 2015).

CyberGuardian HealthTech must comply with HIPAA (Health and Human Services 2024), other data protection laws, and industry-specific standards like Notifiable Data Breaches (RDB)

(OAIC 2024), The Australian Privacy Principles (APP) (OAIC 2024), Health Records Act 2001 (Victorian Legislation 2024), and Prudential Standard CPS 234 (Imperva 2024).

Ransomware attacks, insider threats, third-party vulnerabilities, and data breaches in Electronic Health Records (EHR) systems put the firm at risk of violating strict healthcare regulations. Compliance is crucial for CyberGuardian HealthTech, a healthcare provider, to maintain high ethical standards and trustworthiness. CyberGuardian HealthTech must follow regulations to test, reduce legal hazards, and maintain ethics (Clifton 2024).

An organized strategy may help CyberGuardian HealthTech solve compliance issues (Rhapsody 2024). This includes creating goals, allocating resources, and assigning duties. First, CyberGuardian HealthTech must prioritize data protection, security standards like GDPR (Intersoft Consulting 2024) and HIPAA, and industry regulations due to its healthcare technology focus. Compliance expectations are taught through training and awareness—monitoring and auditing to assess compliance and address noncompliance (SCCE 2024). The firm must always be prepared for incident response and recovery breaches. Establishing a business continuity plan that tackles inadequacies ensures continued operations (Irei 2024). Finally, CyberGuardian HealthTech's business, reputation, and patient welfare depend on strong compliance management.

### 1.3 Risk Management

To do a risk assessment in the healthcare industry, one must first identify all possible threats to the privacy, security, and availability of patient records and other mission-critical infrastructure. A comprehensive risk assessment should be carried out annually by CyberGuardian HealthTech to identify any weak spots and threats. Unauthorised access to data, ransomware attacks, internal threats, and vulnerabilities in externally controlled systems are all part of these types of dangers (LucidChart n.d). Potential risks include, but are not limited to, malware, phishing schemes, insider threats, and system flaws. If there is a risk to data availability, confidentiality, or integrity, an impact review will find out. The likelihood of each risk and the impact it might have on CyberGuardian HealthTech's operations, reputation, and compliance status are two factors that must be considered while evaluating these risks.

The risk treatment plan delineates approaches for mitigating identified risks:

- Risk avoidance (complete elimination of the risk)
- Reduction (implementation of controls to minimize the probability or consequences of the risk)
- Transfer (transferring the risk to a third party through insurance or outsourcing)
- Acceptance (acknowledging the risk without pursuing additional measures).

CyberGuardian must be proactive and flexible in risk management to handle the changing cyber threat scenario. This requires regular risk surveillance and review to ensure that mitigation strategies are effective against new dangers. The company's strategy involves implementing firewalls, intrusion detection systems, and anti-malware solutions in order to safeguard the network. Systematic software updates and patch management will be implemented to reduce the impact of identified vulnerabilities. Cybersecurity training programs aim to educate employees on potential risks and effective strategies for safeguarding data (Axel Sukianto 2024). These programs equip employees with the skills to recognize and report phishing attempts and suspicious activity. A comprehensive incident response plan will be created, detailing the protocols for identifying, controlling, and restoring operations in the event of an occurrence.

## Part 2: Cybersecurity Policy Development

### 1. Organizational Structure for Cybersecurity

#### 1.1 Organizational Chart Clarity

Tipton and Krause argue that a properly organized organizational chart should clearly define roles, reporting lines, and the chain of command, thereby improving coordination and expediting decision-making during times of crisis (Tipton and Krause 2007). CyberGuardian should prioritize the Chief Information Security Officer (CISO) at the top of the organizational chart, emphasizing their strategic responsibility for supervising cybersecurity policies and practices. The primary responsibilities of the Chief Information Security Officer (CISO) encompass the Incident Response Manager, Security Operations Center (SOC) Manager, Compliance Officer, and Vendor Security Assessor. These roles would be associated with teams of analysts, specialists, and engineers, with reporting lines to the Chief Information Security

Officer (CISO) and the corresponding managers. Clarity guarantees that every team member possesses a comprehensive understanding of their duties and their alignment within the broader framework of the organization's cybersecurity endeavors.

## 1.2 Role Alignment and Interactions

CyberGuardian HealthTech's cybersecurity team must unify roles and interactions to improve security and operational integrity. Whitman and Mattord (2018) state that well defined roles and organized interactions help team members understand their roles and contributions to organizational goals. CyberGuardian's Incident Response Manager and SOC Manager should work together to respond to security breaches and threats. The Compliance Officer must regularly interact with these roles to ensure regulatory and business policy compliance. The Vendor Security Assessor works with external partners to manage third-party risks and maintain security standards. Effective communication across these positions enables for a unified cybersecurity strategy that adapts to new dangers and the changing healthcare sector.

## 2. Cybersecurity Policy

### 2.1 Policy Coverage and Relevance

Based on the results of the first phase, CyberGuardian HealthTech must prioritize protecting the authenticity, availability, and secrecy of data and resources that are crucial to our mission. To achieve this, we will implement a comprehensive cybersecurity strategy that covers important aspects such as data protection, user privacy, and incident response.

We will implement role-based access controls (RBAC) to ensure only authorized users can access critical data. Additionally, we will securely manage data throughout its lifespan by defining data retention and disposal protocols and implementing strict access controls to ensure that only authorized workers have access ([Sharon & Alissa 2022](#)).

Our proactive approach to security issues is evident in our developed comprehensive strategy. This strategy outlines specific steps to be taken in the event of an incident, including detection, reporting, and mitigation. We place a high priority on post-incident



analysis to extract valuable insights and enhance our response capacity. These insights will guide the implementation of remedial steps, thereby preventing future incidents of a similar nature (Negrea 2023).

Our policy requires users to follow the concept of least privilege when managing their access to prevent them from accessing unnecessary resources. Secure authentication can be achieved by implementing strong password restrictions, multi-factor authentication (MFA), and frequent training on best practices for access control (Kinza & Mary 2023).

We will regularly evaluate our policies as part of our commitment to maintaining robust security standards. This evaluation will ensure that our policies can adapt to new technology, changes in regulations, and emerging threats. We will also assess the security posture of our partners through vendor risk assessments. Our vendor contracts will include provisions that compel them to follow cybersecurity best practices and promptly disclose security events, ensuring compliance with our security standards and regulatory requirements (Catherine 2024)

## 2.2 Policy Practicality and Enforceability

It is important to highlight the usability and enforceability of cybersecurity measures. Encryption and data classification are standard measures that can be put in place and monitored to ensure they are followed. All businesses that deal with data should have an incident response plan, and it is necessary to rehearse it often and review it when an event occurs. Strong password restrictions and the principle of least privilege can reduce the risk of unauthorized access. Technical tools and audits may be used to ensure that these policies are followed. To minimize third-party risk, it is recommended to perform regular security assessments of third-party providers; contractual penalties and audits may ensure compliance. To ensure that the cybersecurity policy is up-to-date and effective, the policy review committee should enforce it and keep it current. Our rules prioritize practicality, enforceability, and alignment with our business goals to secure our assets and achieve sustainable development in a constantly changing digital world.

### 2.3 Review and Revision Mechanism

Effective cybersecurity requires well-defined mechanisms for assessing and modifying policies often. CyberGuardian HealthTech can organize an IT, legal, HR, and operational Policy Review Committee to do this. The committee should regularly review the cybersecurity policy and conduct further evaluations in response to security breaches, major IT changes, or new requirements. New rules, technology, and severe dangers in cybersecurity should be monitored by the committee. After evaluations, the committee should propose cybersecurity policy revisions to the management team for approval. All staff must be informed and trained on policy changes. If an audit shows policy noncompliance, fix it. By following these instructions, CyberGuardian HealthTech may strengthen its cybersecurity and secure its assets. This flexible policy review and revision technique allows CyberGuardian HealthTech to quickly adapt to new cyber threats and technical developments.

## Referencing

Adedoyin F. & Christiansen B. (2023) Effective cybersecurity operations for enterprise-wide systems. 1st ed. Hershey, PA: IGI Global, accessed April 25 2024.[https://rmitlibraryvn.rmit.edu.vn/permalink/84RVI\\_INST/1kigfja/alma9910013162756068](https://rmitlibraryvn.rmit.edu.vn/permalink/84RVI_INST/1kigfja/alma9910013162756068)  
21

Australian Government Office of the Australian Information Commissioner (2024), Notifiable data breaches, accessed April 24 2024. <https://www.oaic.gov.au/privacy/notifiable-data-breaches>

Australian Government Office of the Australian Information Commissioner (2024), Australian Privacy Principles, accessed April 24 2024.<https://www.oaic.gov.au/privacy/australian-privacy-principles>

Axel Sukianto (2024) 10 Ways to Reduce Cybersecurity Risk for Your Organization, Upguard website, accessed 23 April 2024. <https://www.upguard.com/blog/reduce-cybersecurity-risk>

Catherine C (2024), Vendor Risk Assessments: An Ultimate Guide, 'UpGuard', accessed April 25 2024.<https://www.upguard.com/blog/vendor-risk-assessment>

Clifton D (2024), What is Healthcare Compliance Ethics?, MedTrainer, accessed April 24 2024. <https://medtrainer.com/blog/healthcare-compliance-ethics/>

Health and Human Services (2024), Health Information Privacy', Health and Human Services, accessed April 24 2024. <https://www.hhs.gov/hipaa/index.html>

Imperva (2024), What is CPS 234?, Imperva, accessed April 24 2024.<https://www.imperva.com/learn/data-security/cps-234/>

Intersoft Consulting (2024), General Data Protection Regulation GDPR, Intersoft Consulting, accessed April 24 2024. <https://gdpr-info.eu>

Irei A (2024), What is incident response? A complete guide, TechTarget, accessed April 24 2024. <https://www.techtarget.com/searchsecurity/definition/incident-response>

Kinza Y & Mary E (2023), Multifactor authentication, 'TechTarget', accessed April 25 2024.<https://www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA>

Koop C & Lodge M (2015) ,What is regulation? An interdisciplinary concept analysis, 'Research Gate, accessed April 23

2024.[https://www.researchgate.net/publication/280915642\\_What\\_is\\_regulation\\_An\\_interdisciplinary\\_concept\\_analysis](https://www.researchgate.net/publication/280915642_What_is_regulation_An_interdisciplinary_concept_analysis)

Lucidchart editor (n.d) A complete guide to the risk assessment process, Lucidchart website, accessed 23 April 2024. <https://www.lucidchart.com/blog/risk-assessment-process>

Muhammad F, Muharman L & Hanif F (2023), Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity, 'MDPI', accessed April 25

2024.<https://www.mdpi.com/2071-1050/15/18/13369>

Negrea P (2023), A Comprehensive Analysis of High-Impact Cybersecurity Incidents: Case Studies and Implications, 'ResearchGate', accessed April 25

2024.[https://www.researchgate.net/publication/375062115\\_A\\_Comprehensive\\_Analysis\\_of\\_High-Impact\\_Cybersecurity\\_Incidents\\_Case\\_Studies\\_and\\_Implications](https://www.researchgate.net/publication/375062115_A_Comprehensive_Analysis_of_High-Impact_Cybersecurity_Incidents_Case_Studies_and_Implications)

Rhapsody (2024), A platform for Healthcare IT Innovation, Rhapsody, accessed April 24 2024.

<https://rhapsody.health/resources/platform-healthcare-it-innovation-achieving-your-strategic-objectives/>

SCCE (2024), SCCE Compliance 101 Third Edition, Cosmos, accessed April 24

2024.<https://compliancecosmos.org/chapter-7-monitoring-auditing-and-reporting>

Sharon S & Alissa I (2022), What is data security? The ultimate guide, 'TechTarget', accessed April 25 2024.<https://www.techtarget.com/searchsecurity/Data-security-guide-Everything-you-need-to-know>

Sikdar P (2022), Strong Security Governance Through Integration and Automation : A Practical Guide to Building an Integrated GRC Framework for Your Organization, accessed April 25

2024.<https://ebookcentral.proquest.com/lib/rmit/reader.action?docID=6797767&ppg=54>

Tipton HF and Krause M (2007) Information Security Management Handbook, CRC Press, doi:<https://doi.org/10.1201/9781439833032>.

Victorian Legislation (2024), Health Records Act 2001, Victorian Legislation, accessed April 23

2024.<https://www.legislation.vic.gov.au/in-force/acts/health-records-act-2001/049>

Volchkov, A 2018, Information Security Governance : Framework and Toolset for CISOs and Decision Makers, accessed April 25 2024.[https://rmitlibraryvn.rmit.edu.vn/permalink/84RVI\\_INST/1kigfja/alma9910013162756068](https://rmitlibraryvn.rmit.edu.vn/permalink/84RVI_INST/1kigfja/alma9910013162756068)  
21

Whitman ME and Mattord HJ (2018) Principles of information security, 7th edn, Cengage Learning, Boston, Mass.

Lucidchart editor (n.d) *A complete guide to the risk assessment process*, Lucidchart website, accessed 23 April 2024. <https://www.lucidchart.com/blog/risk-assessment-process>

Axel Sukianto (2024) *10 Ways to Reduce Cybersecurity Risk for Your Organization*, Upguard website, accessed 23 April 2024. <https://www.upguard.com/blog/reduce-cybersecurity-risk>

**Frist class**  
**ASSIGNMENT SERVICE**  
that you deserve



**ƯU ĐÃI 25% CHO FIRST ORDER**

Tận hưởng trải nghiệm học tập với DrKhanh Assignment. Đặt hàng ngay hôm nay để nhận được sự hỗ trợ chuyên nghiệp và đạt được thành công trong học tập của bạn!

**▶ NHẬN TƯ VẤN MIỄN PHÍ! ◀**

Đừng ngần ngại liên hệ với đội ngũ của chúng tôi nếu bạn cần bất kỳ thông tin bổ sung nào hoặc muốn biết thêm về dịch vụ của chúng tôi. Chúng tôi luôn sẵn lòng hỗ trợ bạn!



