IN-COURSE ASSESSMENT (ICA) SPECIFICATION

Module Title: **Information Governance**	Module Leader: **V Rushin-Chape** Module Code: **CIS3005-N**
Assignment Title: **Information Governance Portfolio**	Deadline Date: **Friday 2nd May 2025** Deadline Time: **4:00pm** **Submission Method:** Online (Blackboard) ☑ Middlesbrough Tower ☐

Online Submission Notes:

- Please carefully follow the instructions given on the Assignment Specification.
- When an extension has been granted, a fully completed and agreed Extenuating Circumstances form must be used.

Library Support for Academic Skills:

Did you know you can book an individual 30 minute tutorial in the Learning Hub with an adviser to help you with your academic skills, writing or numeracy? Or that there are loads of really useful workshops available to help you with your studies and assessments? Have a look at the Succeed @ Tees workshops for more details.

FULL DETAILS OF THE ASSIGNMENT ARE ATTACHED INCLUDING MARKING & GRADING CRITERIA

Information Governance Portfolio

This assessment constitutes 100% of the overall module mark. Please read the whole document to fully understand the assessment requirements.

If you are undertaking this module as part of a Higher Degree Apprenticeship (i.e. BSc (Hons) Digital and Technology Solutions) please speak directly with your Module Leader to determine whether your workplace has a suitable case study that could be used for this assessment.

Case Study

My_hEalth

Fitness trackers and monitors have become increasingly popular and play an important part in aiding the everyday person to become responsible for their own health and fitness. According to Fortune Business Insights, in 2020 the global fitness tracker market was worth over £29billion and is forecast to grow to over £91billion by 2028.

The owner of ***My_hEalth*** has realised that there is a gap in the market for an effective data integration app which provides a visually attractive interface for health and fitness related metrics that can be collected from a multitude of devices. There is currently a competitive race to be the first to bring such a well integrated application to the market, and it needs to work on all mobile platforms in addition to being able to collect data from all popular devices and existing software providers, including FitBit, Garmin, Whoop, Google Fit, Apple, MyFitnessPal and many more. The owner is aiming for the application to be able to prompt the wearer at key points (e.g. “Drink more water!” or “You need to rest today” etc.) as well as provide the ability to automatically send health related data to healthcare professionals and insurers.

Its unique selling point will be the industry-leading integration and sharing, which relies on data integrity, availability, accuracy etc. and must be very carefully protected in order to comply with legislation. The application is in the late stages of development and has been created securely by design through collaboration with industry experts. The owner has invested very large sums of personal money, and there are early investors pushing for a strict release deadline. The app will offer a limited free service but for full integration and insights customers will need to pay a monthly subscription. A small portion of this monthly fee will be paid back to the partner manufacturers/software providers in return for the ability to use their data.

Currently the development team is small (8 people). However, the owner now needs to step up production in order to hit the agreed deadlines, and has decided to extend the team by employing another four full time developers and a sales and marketing lead who also has good experience in data security.

To date the team have been working from home but once the team expands they will need to locate to a central office where they can work together, although it is intended that working from home will be permitted for a proportion of the working week.

Encouraging manufacturers to share data for testing the app integration has been very challenging, and some have expressed a concern that the data governance of ***My_hEalth*** is not as transparent or robust as it should be, and as a result have been reluctant to share real data. Moving forward, the team have been advised to produce a set of key documentation and processes to reassure partner manufacturers. In addition, one of the largest investors has also expressed a concern over similar issues and has threatened to withdraw their funding. The lure of such an exciting application has kept them interested to this point, and the team need to act fast.

The team have already taken some initial cyber security training but they understand more will be required. There is also a need to ensure a formal audit trail of processes, responsibilities and operations.

It is intended that the application will import/collect, process and store the following types of data:

- Heart rate
- Heart rate variability
- Resting heart rate
- Peak heart rate
- Average heart rate
- Heart rate zones
- Calories consumed
- Calories burned
- Sleep metrics (time, type (e.g. REM, light etc.)
- Activity type (including recovery such as massage therapy)
- Activity time
- Location
- Ambient temperature
- Skin temperature
- Respiration rate
- Weight
- Body mass
- Steps
- Distance travelled (e.g. run, walk, cycle, swim etc.)
- GPS route data
- Floors climbed
- Intensity minutes
- Day strain level
- Morning recovery level
- Day stress level
- Menstrual tracker
- Water consumed
- Vitamins/minerals consumed
- Blood oxygen level
- Postural data (if a web cam is connected whilst working at a desk)
- Usual sleep and wake times
- Usual eating times
- Device type and location (e.g. wrist band)
- Profile information (e.g. date of birth, address etc.)
- Timezone
- IP address
- Location

It is intended that healthcare reports will/could utilise all of the above data and the team would like to ensure that the ability to collect additional data (expand data types etc.) is already built into the design of the application.

You may need to make a number of assumptions for this case study, so you must ensure that you include these in your assessment to help justify your decision making.

Assessment Requirements

Your task is to put together the following items for the case study company (in total around 4000 words):

1. A risk assessment analysis relating to data security and your recommendations for risk mitigation to ensure business continuity. **[25 marks]**
    - Guide: 1200 words
    - To include identified risk name, description, likelihood and severity, overall risk score, specific mitigation with justification linked to business continuity
    - All risks should be clearly related to this scenario. You may need to limit the range of risks in your discussion to meet the word count – aim for a minimum of 8 in detail.

2. A summary of ethical, social, legal and regulatory compliance issues relating to this case study, to include clear information on all applicable laws and industry best practice (such as ISO27K). The summary should demonstrate an understanding of the differences between ethical and legal considerations. It should include a clear list of controls you plan to implement with justification for each. **[35 marks]**
    - Guide: 2000 words
    - To include a comprehensive list of all pertinent legislation and ethical and social issues with clear controls identified and justified
    - To include clear links between issues identified, suggested controls and associated legislation/standards
    - To include an indication of consequences to the organisation in the event of non-compliance

3. An A4 electronic poster showing the steps to be taken for Disaster Recovery. It should indicate responsibilities and have a clear start and end. This process is to be followed by your IT team in the event of an IT related disaster. **[20 marks]**
    - Guide: 200 words (mostly design but some explanatory text could be present)
    - Should be relevant to the target audience
    - Should be **generic** enough to be followed in the event of **any** IT/data related disaster
    - Use formal process flow notation

4. A reflection on the portfolio you have produced: its strengths and weaknesses and your own learning based on your degree route. **[10 marks]**
    - Guide: 600 words
    - The reflection needs to be honest and identify areas for improvement within the portfolio, with justifications

- You can reflect on every aspect of the portfolio you have produced, including presentation, your recommendations, content, references, time management etc.
- It should link to your prior learning, and future career choice

5. The entire portfolio needs to be professionally presented and suitable for the target audience (case study company). **[10 marks]**
    - References should be included in appropriate places
    - It should be free from major spelling/grammatical issues and in a publishable state
    - It should include page numbers, a table of contents, sensible headings, list of references and appendices (if appropriate).
    - The structure should be easy to follow and logical
    - Any assumptions should be listed throughout

Hand in Requirements

Please upload your portfolio as one document to Blackboard by the deadline, in .pdf format. Include the word count on the cover page.

How this module is assessed

This module assessment covers all the module learning outcomes, and Higher Degree Apprenticeship Knowledge, Skills and Behaviours (KSBs) as detailed below:

Learning Outcomes (applies to Undergraduate Degree and Higher Degree Apprenticeships)

Personal & Transferable Skills

1. Critically evaluate a data governance implementation plan created for a specified business need and reflect on any potential changes and improvements with regard for impact, quality and trade-offs.
2. Communicate effectively and professionally in order to present arguments clearly.
3. Demonstrate a comprehensive and detailed knowledge of the goals and principles of information governance and what it means to work ethically and professionally in accordance with these goals and principles.

Research, Knowledge & Cognitive Skills

4. Demonstrate an understanding of the legal frameworks and international standards underpinning information governance.
5. Design an appropriately researched data governance implementation plan appropriate for a specified business need that includes business continuity and disaster recovery planning.
6. Be able to advise on, and evaluate, the ethical and social issues arising from security measures used by business.
7. Demonstrate a complex understanding of the breadth and depth of the physical and environmental security issues for a given scenario and demonstrate a critical awareness of current problems and issues informed by research findings and professional practice.

Professional Skills, Values and Behaviours

8. Provide professional advice and guidance on legal and regulatory compliance.
9. Plan, analyse and evaluate a risk management framework and recommend appropriate operations security measures.

Knowledge, Skills and Behaviours (applies to Higher Degree Apprenticeship only)

This module maps to the following BSc (Hons) Digital and Technology Solutions Degree Apprenticeship KSBs, in accordance with the Degree Apprenticeship Standard for the ***Software Engineer*** and ***Cyber Security Analyst*** specialisms:

KSB	Description

C1	Is able to critically analyse a business domain in order to identify the role of information systems, highlight issues and identify opportunities for improvement through evaluating information systems in relation to their intended purpose and effectiveness
C4	can undertake a security risk assessment for a simple IT system and propose resolution advice. Can identify, analyse and evaluate security threats and hazards to planned and installed information systems or services (e.g. Cloud services).
C5	can apply organisational theory, change management, marketing, strategic practice, human resource management and IT service management to technology solutions development. Develops well-reasoned investment proposals and provides business insights.
C6	follows a systematic methodology for initiating, planning, executing, controlling, and closing technology solutions projects. Applies industry standard processes, methods, techniques and tools to execute projects. Is able to manage a project (typically less than six months, no inter-dependency with other projects and no strategic impact) including identifying and resolving deviations and the management of problems and escalation processes.
C7	can plan, design and manage computer networks with an overall focus on the services and capabilities that network infrastructure solutions enable in an organisational context. Identifies network security risks and their resolution.
C13	Common vulnerabilities in computer networks including unsecure coding and unprotected networks.
C14	The various roles, functions and activities related to technology solutions within an organisation.
C16	How to deliver a technology solutions project accurately consistent with business needs.
C17	The issues of quality, cost and time for projects, including contractual obligations and resource constraints.
C18	Fluent in written communications and able to articulate complex issues.
C24	Applies analytical and critical thinking skills to Technology Solutions development and to systematically analyse and apply structured problem-

	solving techniques to complex systems and situations.
C26	Able to conduct effective research, using literature and other media, into IT and business-related topics.
C29	Ability to perform under pressure
C30	A thorough approach to work

In addition, this module maps to the following BSc (Hons) Digital and Technology Solutions Degree Apprenticeship KSBs, in accordance with the Degree Apprenticeship Standard for the ***Cyber Security Analyst*** specialism:

KSB	**Description**
CS1	Analyse and evaluate security threats and vulnerabilities to planned and installed information systems or services and identify how these can be mitigated against
CS2	Perform security risk assessments for a range of information systems and propose solutions
CS3	Develop a security case against recognised security threats, and recommend mitigation, security controls and appropriate processes
CS4	Define and justify a user access policy for an information system given knowledge of the system architecture, security requirements and threat/risk environment. This should be in terms of what they can do, resources they can access, and operations they are allowed to perform
CS5	Perform a business impact analysis in response to a security incident and follow a disaster recovery plan to meet elements of a given business continuity policy
CS7	The types of security (confidentiality, authentication; non-repudiation; service integrity) and security big picture (network security; host OS security; physical security)
CS8	The main types of common attack techniques, including phishing, social engineering, malware, network interception, blended techniques, denial of service and theft
CS9	How to recognise and assess risk including performing a risk assessment
CS11	The different approaches to risk treatment and management in practice

CS12	What the ‘cyber security culture’ in an organisation is, and how it may contribute to security risk

Marking Criteria

Part	*Criteria*		*Marks*
Item 1 Risk Assessment	70% +	Excellent work to an extremely high professional standard which covers all conceivable risks. Descriptions are highly detailed and include excellent appropriate information. May exceed expectations at this level.	25%
	60-69%	Very good work to a professional standard which covers a wide range of risks. Descriptions are detailed and include very good appropriate information.	
	50-59%	Good work to a reasonable professional standard which covers a range of conceivable risks. Descriptions are reasonable and include appropriate information.	
	40-49%	An attempt has been made to identify appropriate risks but there are some missing and/or they are not appropriate. Descriptions are included but are not always appropriate or lack detail.	
	<40%	A poor attempt which does not meet the module learning outcomes. It may have missing information or has missed the point.	
Item 2 Controls	70% +	Excellent summary to an extremely high professional standard. Includes excellent detail. It could be implemented in industry. May exceed expectations at this level.	35%
	60-69%	Very good summary to a professional standard. Includes good detail. Could be implemented in industry with some minor adjustments.	
	50-59%	Good summary to a reasonable professional standard. Includes reasonable detail. It could be implemented in industry with more work.	

	40-49%	An attempt has been made to write a summary. Details have been included but are not clear or have no meaning in this context. The document is somewhat vague and needs quite a lot more work.	
	<40%	A poor attempt which does not meet the module learning outcomes. It may have missing information or has missed the point entirely.	
Item 3 Disaster Recovery Poster	70% +	An excellent informative poster which includes an excellent process flow diagram with references. The steps are logical, realistic and accurate.	20%
	60-69%	A very good poster which includes a very good process flow diagram and references. The steps are accurate and logical.	
	50-59%	A good poster with a reasonable process flow diagram (may have missing points) and references. There may be some minor errors present but it's mostly accurate and logical.	
	40-49%	A poster has been submitted but it lacks detail and the process flow diagram may be too simple or incorrect, or missing. Referencing is present but could be improved. Steps could be more accurate and logical.	
	<40%	A poor attempt which does not meet the module learning outcomes. It may have missing information or has missed the point entirely.	
Item 4 Reflection	70% +	An excellent reflection which identifies strengths and areas for improvement with detailed reasoning. Professional layout and could be published. It clearly links the current module learning to prior learning and experiences and considers future learning and/or career choices in detail. Incorporates references and/or best practice examples.	10%
	60-69%	A very good reflection which identifies a number of strengths and areas for improvement with some reasoning. Layout is good enough to publish with minor amendments. It links learning experiences well and includes references.	

	50-59%	A good reflection with a selection of points raised. It could be more reflective and make use of references. There is some linking of learning experiences. There may be some minor errors present. Reasonable layout but needs more work.	
	40-49%	A reflection has been written but it lacks detail and does not provide justifications. No linking of learning experiences included. Layout could be improved, and it needs more work.	
	<40%	A poor attempt which does not meet the module learning outcomes. It may have missing information or has missed the point entirely.	
Professional Presentation	70% +	Presentation is excellent all round and makes use of industry-appropriate language. All items could be implemented in industry.	10%
	60-69%	Presentation is very good and could be implemented in industry with minor amendments.	
	50-59%	Presentation is acceptable but may lack some of the requirements listed in the specification.	
	40-49%	Presentation could be improved based on the requirements listed in the specification.	
	<40%	A poor attempt which does not meet the module learning outcomes. It may have missing information or has missed the point entirely.	