Diploma Programme
Programme du diplôme
Programa del Diploma

Markscheme

May 2019

Information technology in a global society

Higher and standard level

Paper 2

17 pages

Using assessment criteria for external assessment

For external assessment, a number of assessment criteria have been identified. Each assessment criterion has level descriptors describing specific levels of achievement, together with an appropriate range of marks. The level descriptors concentrate on positive achievement, although for the lower levels failure to achieve may be included in the description.

Examiners must judge the externally assessed work at SL and at HL against the four criteria (A–D) using the level descriptors.

- The same assessment criteria are provided for SL and HL.
- The aim is to find, for each criterion, the descriptor that conveys most accurately the level attained by the candidate, using the best-fit model. A best-fit approach means that compensation should be made when a piece of work matches different aspects of a criterion at different levels. The mark awarded should be one that most fairly reflects the balance of achievement against the criterion. It is not necessary for every single aspect of a level descriptor to be met for that mark to be awarded.
- When assessing a candidate's work, examiners should read the level descriptors for each criterion until they reach a descriptor that most appropriately describes the level of the work being assessed. If a piece of work seems to fall between two descriptors, both descriptors should be read again and the one that more appropriately describes the candidate's work should be chosen.
- Where there are two or more marks available within a level, examiners should award the upper marks if the candidate's work demonstrates the qualities described to a great extent. Examiners should award the lower marks if the candidate's work demonstrates the qualities described to a lesser extent.
- Only whole numbers should be recorded; partial marks, that is fractions and decimals, are not acceptable.
- Examiners should not think in terms of a pass or fail boundary, but should concentrate on identifying the appropriate descriptor for each assessment criterion.
- The highest level descriptors do not imply faultless performance but should be achievable by a candidate. Examiners should not hesitate to use the extremes if they are appropriate descriptions of the work being assessed.
- A candidate who attains a high level of achievement in relation to one criterion will not necessarily attain high levels of achievement in relation to the other criteria. Similarly, a candidate who attains a low level of achievement for one criterion will not necessarily attain low achievement levels for the other criteria. Examiners should not assume that the overall assessment of the candidates will produce any particular distribution of marks.
- The assessment criteria must be made available to candidates prior to sitting the examination.

Theme: Business and employment

Background information:

Please read carefully as the students may rely on this knowledge that is not specified in the article.

The exam is not a technical one on RFID.

Some students will have studied RFIDs in detail, and some will not, but the transfer of knowledge of other similar systems to this system will be positively marked, ***even if the transfer is not technically correct.*** *This applies especially to the developments in Question 2a and the technical solutions in Question 4.*

The system in the article seems to imply that it is one can have significant storage and transmission capabilities, e.g. 'read the data' (line 11), may be passive or active RFID, the amount and type of 'data' is not specified but seems to be significant, 'RFID chip containing their personal information' (line 3, 17)

I*mportant Information: especially about GPS and chips that students may be confused about for Q2a or Q4:*

http://www.bbc.com/capital/story/20170731-the-surprising-truths-and-myths-about-microchip-implants

Passive and active RFID

https://blog.atlasrfidstore.com/active-rfid-vs-passive-rfid

Storage capacity of RFID

http://www.asiarfid.com/rfid-basics/how-much-information-can-rfid-card-store.html

Criterion A — The issue and stakeholder(s) **[4]**

1. (a) Describe **one** social/ethical concern related to the IT system in the article.

***[1]**: for identification of the concern (which may not be explicitly named or incorrectly named or vaguely named).*
***[2]:** there needs to be an explicit description of the impact/result/consequences/effect/outcome on the employee/company. If the description is clear but does not contain a specific identification like privacy or security still award two marks. The question asks for the concern to be described. If two linked/overlapping concerns are identified eg privacy and security, mark the best response and that concern needs to be explained in (2)(b).*

The description needs to reference the IT system in the article.

*If **two** different concerns are raised, only mark the first since the question specifies **one** concern; except if commonly linked eg security and privacy.*

Social/ethical concerns may include the following:

Be aware that the students may confuse privacy and security – if a clear concern but confused between privacy and security award 1 mark.

If you are unsure about the social/ethical concern identified by the candidate and believe it should be in the markscheme, please contact your Team Leader.

Privacy concerns - privacy breach is access to information without owner's consent

- unauthorised people reading/accessing the employee's stored information
- employer may use the data for other unintended purposes if there is no policy in place to control use – refer to privacy laws
- possible tracking of the employees within the company building
- ongoing privacy of the employee – who has access to the data (or who may gain access to it in the future) and what could they do with it
- personalization of the chip for broader purposes by employee – ability for employee use the unique RFID as a identifier for other facilities etc
- the employee must sign a contract to allow the chip to be implanted by the company and the employee feels vulnerable as he or she is afraid to lose the job if they do not sign the contract.

Security concerns - security breach is un-authorised access to information through illegal technical or other means

- security of an employee's personal data on the chip
- security of the employee's personal data sent to/stored by the company
- security of the employers' premises and equipment if a chip malfunctions.
- Security – physical – of person with valuable data and chip implant that others want

Reliability concerns

- reliability of the data stored on the chip and/or the company database. The stored data may be out-of-date
- reliability of the system/network infrastructure. If the system malfunctions, people may be denied access to legitimate areas/resources or possibly allowed access to areas/resources for which they are not authorized

- microchips can cause medical problems and may interfere with medical scans e.g. MRI and security at airports
- repurposing of the chip after employment finishes.
- portability of the unique identifier within the chip beyond the company – standards
- multiple RFIDs in a hand interfering with each other, or in clothes
- ethical and religious concerns about the implant into the body
- also, other concerns about implants in humans, medical and psychological – the concern of people and machines. Need to ensure that it does not relate to hypotheticals too far into the future (e.g. cyborgs)
- employee leaving/terminated from employment – removal (invasive surgery even if minor)
- ownership of the chip – who does own it the company or employee - Company enforcing removal of chip from departing employee
- chip may become degraded over time causing it to not respond with correct data.

(b) Describe the relationship of **one** primary stakeholder to the IT system in the article.

Describe means to include who, what and where but not how and why for full marks.

***[1]**: who – identification of the stakeholder.*

***[2]**: where and what – 'what' the stakeholder does with the IT system, 'where' would usually be the chip itself or the associated IT systems.*

Primary stakeholders may include the following:

- the employee who has the chip implanted
- the employer/company responsible for issuing the chips/ supporting the technology
- the employee must be authorised by the company's IT system to gain access to company resources.
- Technical person responsible for maintaining the system – not a primary stakeholder unless described as such by student in a meaningful way
- The medical personal responsible for the embedding (and potential removal) procedures - Not primary in day to day operation by is primary in the implementation of the IT system.

Marks	***Level descriptor***
0	*The response does not reach a standard described by the descriptors below.*
1	*Either an appropriate social/ethical concern **or** the relationship of one primary stakeholder to the IT system in the article is identified.*
2	*Either an appropriate social/ethical concern **or** the relationship of one primary stakeholder to the IT system in the article is described **or** both are identified.*
3	*Either an appropriate social/ethical concern **or** the relationship of one primary stakeholder to the IT system in the article is described; the other is identified.*
4	*Both an appropriate social/ethical concern **and** the relationship of one primary stakeholder to the IT system in the article are described.*

Criterion B — The IT concepts and processes **[6]**

2. (a) Describe step-by-step, how the IT system works.
IT system: Radio frequency identification (RFID) chip implants for employees.

Many of the responses will not fit neatly into a mark descriptor, so best fit will need to be applied.

***[1]**: the student may show some understanding of the process but not in a step-by-step approach – using the information in the article and possibly some steps missing.*

***[2]**: the student is able to provide a logical step-by-step account using the information in the article but lacks some details. Best fit if the answer contains developments/information beyond the article but not in a step-by-step approach. Must contain at least TWO of the major steps below.*

***[3]**: the student is able to provide a step-by-step account which may be detailed. Expect at least TWO major steps plus at least TWO developments.*

***[4]**: at least four technical developments and all the major steps in detail.*

Major steps provided in the article are:
- the RFID scanner reads the data from the chip
- the IT system authenticates the employee
- the IT system confirms that the employee is authorised to perform the requested action and/or the action is performed.

Answers in the article:
- RFID in door connect to lock
- RFID scanner/readers in equipment including photocopiers and computers.

Answers with additional information to that in the article may include the following:
- when the chip is first implanted, employees must register their chip with the company, and each contains a unique RFID number
- the unique RFID number is added to the database (as the primary key or other field of the employee's record), along with other relevant details of the employee
- when the employee passes their hand near a scanner, the electrical energy from the scanner provides power to activate the chip and transmit its data
- scanner reads the unique ID number of the RDIF chip (and the other personal information) from the data received
- the ID number is sent to a database where it is matched with the unique chip RFID number in the employee table to retrieve the employee record
- the system also checks if the employee is permitted to perform the requested action (*eg* unlock a door)
- if the ID number matches a stored number and the action is permitted, the system sends back a confirmation to the equipment to perform/allow the employee to perform the requested action
- if the ID number is not found or the requested action is not permitted, the system denies access.
- system may record time of attempted access or access to resource
- cost of the lunch is read from the keyboard or barcode scanner
- employee's RFID number is matched in the database to retrieve employee's record

- add the lunch cost to the employee's record
- beep sound to confirm chip has been used – beep by scanner
- the RFID implant is passive (has no energy source of its own) and get activated when it is in proximity to a RFID scanner
- details such as: a list of actions the employ is allowed to do (unlock the door, permitted to enter store room, etc) stored in company servers
- electromagnetic energy from the scanner continuously emits radio signals at a particular wave length that activates any chip in the near vicinity
- volume of data stored on RFID chip is usually up to 2KB – often just unique identifier.

(b) Explain the relationship between the IT system and the social/ethical concern described in **Criterion A**.

Explaining the link between the concern and specific parts, or whole, of the IT system means the student must include how and why the concern has arisen from the use of the IT system. The naming of the concern identified in Criterion A may be implicit.

Q2(b) clearly asks for a link to Q1(a), but the link only needs to be generic – eg for a specific security concern described in Q 1(a), then in Q2(b) the student can explain a security weakness without reference to the specific concern in Q1(a).

*If the concern addressed in Q2(a) is completely different from that in Q1(a) a link cannot be made and hence **[0]**.*

Q2(b) can also be related back to Q1(b) where the who and what and where of the IT system usage are described.

***[1]**: if the student identifies the relationship between the concern and the IT system. This may be a repeat, or rewording, of the response to (1)(a) or lack detail for the how and why.*

***[2]**: how and why the concern can happen must be described: eg privacy: responses need to specify how (technical) the data can be accessed (similar to some of the steps for 2(a)) and why it has been allowed to be accessed (eg lack of privacy settings – technical weakness).*

Relationship of the IT system to privacy issues:

Unauthorised people reading/accessing the employee's stored information

- (how) data stored on the chip and/or the company database may be accessible to unauthorised (why) people inside or beyond the company.

- (how) employee concerned about losing job and/or their privacy (why) The employee must sign a contract to allow the chip to be implanted by the company and the employee feels vulnerable as he or she is afraid to lose the job if they do not sign the contract.

Possible tracking of the employees within the company building

- (how) with suitably place scanners the implanted chip would allow the company to track the location of the employee as they move around the company building. (Why) this could be done without the employee being aware that they are being monitored. By logging date/time of door access, lunch payments the employee may be able to calculate time spent in the office/away from the desk.

Potential to track employee beyond the company

- (how) RFID readers/scanners in public places (or other company buildings) could allow people to be identified and tracked (through time/date logs) even when they are not inside the company buildings, without the person being aware that this is happening. (why) The RFID is not secured and is easily accessed by a person with a scanner.

Relationship of the IT system to security issues:

Security of the data on the chip
- the chip can be read by any reader/scanner that is close enough, whether that is legitimate (eg owned by the company) or not. (Why) the RFID is not secured and is easily accessed by a person with a scanner.

Security of the data sent to/stored by the company
- (how) data may be vulnerable to interception during transmission from the chip to the reader or within the company network. (Why) data stored in the database may be insecure/vulnerable. A breach of database security might yield information (*eg* RFID number of senior employee) that would allow a malicious party to gain access to the company buildings/equipment.

Security of the employers' premises and equipment
- (how) a compromised/cloned chip could allow unauthorised persons to access sensitive areas, materials or equipment as the RFID scanner/reader works solely on the permissions stored on the chip and/or by matching the ID number of the chip to the permissions stored on in the database. (Why) The RFID is not secured and is easily accessed by a person with a scanner.

Relationship of the IT system to reliability issues:

Reliability of the data stored on the chip and/or the company database
- (how) unless a change in access permissions is recorded on the company database (and/or updated by re-writing the information stored on the chip itself), (why) the system will become unreliable in terms of granting the correct permissions to the correct employee(s).

Reliability of the system/network infrastructure
- (how) if the system malfunctions/RFID number misread), (why) people may be denied access to legitimate areas/resources or possibly allowed access to areas/resources for with they are not authorised.

Further usage of the unique ID
- (how) some people having multiple RFID embedded with potential interference or misreading issues as several chips are energized at once. (why) RFID chip uses a bespoke/different identifier then the chip may not be able to be used in other systems or if the company restricts access to use the RFID identifier in other system.

Ownership of the chip.
- (how) the RFID chip is provided as by the company and is required as an access tool within the company structure. The chip is embedded within an employee which raises the issue when the employee leaves they may be able to come back. (why) chip has not been deactivated in the database when employee leaves the chip has not been removed.

Candidates are expected to make reference to relevant stakeholders, information technologies, data and processes. Candidates will be expected to refer to "how the IT system works" using appropriate IT terminology.

Marks	***Level descriptor***
0	*The response does not reach a standard described by the descriptors below.*
1–2	*There is little or no understanding of the step-by-step process of how the IT system works and does not go beyond the information in the article.* *The major components of the IT system are identified using minimal technical IT terminology.*
3–4	*There is a description of the step-by-step process of how the IT system works that goes beyond the information in the article.* *Most of the major components of the IT system are identified using some technical IT terminology.* *The relationship between the IT system referred to in the article and the concern presented in criterion A is identified, with some use of ITGS terminology.*
5–6	*There is a detailed description of the step-by-step process that shows a clear understanding of how the IT system works that goes beyond the information in the article.* *The major components of the IT system are identified using appropriate technical IT terminology.* *The relationship between the IT system referred to in the article and the concern presented in criterion A is explained using appropriate ITGS terminology.*

Criterion C — The impact of the social/ethical issue(s) on stakeholders [8]

3. Evaluate the impact of the social/ethical issues on the relevant stakeholders.

Impact = result/consequence/effect/outcome on stakeholder.

There are a number of impacts that can be compared and critically analysed. Given the time constraints not all are needed. At least two stakeholders are required for entrance into the top markband.

***[1]:** one or two impacts identified.*

***[2]:** more than two impacts described of either type – positive or negative.*

***[3]:** analysis by structure – division into groups eg positive/negatives and/or various stakeholders.*

***[4–5]:** must include linking analytical connections (between positive/negatives, various stakeholders, various issues) and/or added evaluative comments about the implications for stakeholders. Students who have supplied a good conclusion apply best fit here. Only one stakeholder, maximum of **[4]** if includes analysis and evaluations, eg the impacts on the learner only. If significant number of impacts but unbalanced for a 6 then best fit for a 4 or 5 depending on the amount of analysis and evaluation.*

***[6]:** recommend at least two negative and two positive impacts for each stakeholder in order to provide a balanced analysis in the top markband. Quality of analysis is the most important consideration.*

***[7–8]:** a conclusion backed by direct reference to the impacts described is needed. The evaluation should focus on the overall impact on all the stakeholders mentioned discussing the balance between the positive and negative impacts.*

Positive impacts may include:

For the employee

- convenience – no need to carry ID cards, remember PIN codes or passwords etc.
- speed – authorisation happens very fast, no need to stop and wait
- less potential risk than using biometrics – if the chip is compromised then it can either be re-programmed or replaced, unlike biometrics which cannot be changed
- employee may be able to use the Unique RFID with other IT systems and applications beyond the company - I.e. home automation, keyless entry to cars.

For the company

- allows for fine-grained control of who is authorised to do what (*eg* employees can be granted access to some areas in the company while being denied access to others)
- easy to keep records of who does what, when and where for auditing, cost control
- chip can potentially be used for an increasing range of purposes in the future
- elimination of passwords/PINS removes the problems caused by employees using weak passwords/writing them down to help them remember/having PINs viewed by other employees while entering them/employees sharing passwords – thus potentially increasing company security
- once inserted may need less IT support than passwords which are often forgotten and need to be changed by IT staff.

Negative impacts may include:

For the employee

- some employees may be particularly opposed/fearful about the implantation process or have cultural/religious/medical/health objections to it
- physical security threat if a person cuts out the chip from the hand or physically assaults a person and forces them to use their hand
- the employee may lose his job if refuses the implantation of the chip / lack of autonomy or choice for the employee
- once implanted, the chip is always there and always “on”. Employees may have little control over how the data on the chip, or records of use of the chip (within the database), is used by the company and/or third parties
- the company can monitor the employee in real-time to locate the employee, and also use the records for the same purpose e.g. monitoring how often the employee has entered the toilet or the coffee room. This is a privacy/surveillance issue
- the data on the chip may be compromised by a malicious third party. The employee may unwittingly allow a third party to be falsely identified as the employee/access sensitive areas – who will be held responsible for this breach?
- removal and or deactivation (data erasure if used beyond unique ID) on termination of employment - traumatic, invasive procedure
- if RFID is used beyond the company - I.e. personal use deactivation might be a problem
- life span of the technology – obsolescence may require further chips leading to potential problems may arise if personal information on the chip is out of date and needs updating. This is difficult as the RFID chip would need to be removed
- incorrect data in the chip could have consequences for access to the system and medical/financial implications – and also medical if the chip needs replacing.

For the company

- an employee’s chip may be compromised (*eg* cloned or the data from it skimmed by a malicious third party), company security may be at risk
- the company would have to offer ongoing support to ensure that permissions were kept updated and data was reliable
- if the employee became the victim of fraud through the use of the chip, would the company be liable for the consequences?
- being forced to have a chip implanted may deter employees from joining the company and cause some employees to leave
- reputation/publicity of the company may suffer due to the possible surveillance of employees / negative publicity
- there may be issues when an employee is fired or resigns. Although their account on the database would be cancelled there is also the issue of extracting the RFID device from their hands
- cost of implanting the chip and other costs associated with the production of medical viable chips may be large. And also, much more than a normal ID tag
- complications due the implants would entail costs for the company (medical and hospital) and, also their insurance companies
- issues with interference with metal and water limiting effectiveness particularly with low and high frequency chips with limited range
- life span of the technology – ongoing investment and upgrade particularly if employee need new chips to operate with newer equipment.

Marks	***Level descriptor***
0	*The response does not reach a standard described by the descriptors below.*
1–2	*The impact of the social/ethical issues on stakeholders is described but not evaluated. Material is either copied directly from the article or implicit references are made to it.*
3–5	*The impact of the social/ethical issues on stakeholders is partially analysed, with some evaluative comment. Explicit references to the information in the article are partially developed in the response. There is some use of appropriate ITGS terminology.*
6–8	*The impact of the social/ethical issues on stakeholders is fully analysed and evaluated. Explicit, well developed references to information in the article are made appropriately throughout the response. There is use of appropriate ITGS terminology.*

Criterion D — A solution to a problem arising from the article **[8]**

4. Evaluate **one** possible solution that addresses at least **one** problem identified in **Criterion C**.

[1]*: solution is identified.*

[2]*: solution is described (what, who, where) and the link to article may be implicit, which could be a general description eg general policy description similar to that found in a textbook.*

[3]*: the solution is applied to the problem directly and not generally (a textbook description would lose this mark, especially encryption) – how and why it solves the problem (first positive evaluation). The solution must be feasible and can be applied to the problem, even if not good "quality".*

[4–5]*: at least one more positive evaluation and at least one negative evaluation is required. Best fit if description is limited.*

[6]*: fully evaluated strengths and weaknesses requires a balance of at least two positive and negative evaluations.*

[7–8]*: concluding paragraph directly referencing the evaluations. Students may propose future developments as part of the conclusion instead of discussion of evaluations – best fit applies.*

Answers may include but are not limited to the solutions listed below. The examiner must use his/her judgment and knowledge to determine if a solution applies to the problem and is feasible. If in doubt the examiner should consult with their Team Leader.

Technical solutions

Encryption

Please note many candidates tend to write boilerplate solutions for encryption.: encryption of the data on the chip and/or in the database - needs to explain how it is encrypted and how it is used to solve the problem or else loses marks for lack of description and inability to explain how it is applied to solve the problem.

- personal data being transferred is encrypted to prevent packet sniffing of the data during transfer – A key is held within the database for authorised decryption
- the RFID only contains a unique identifier that is linked to the database – personal data is secured within the database.

Data Integrity

- incorrect data in the chip – implementation of data validation and data verification processes on the database and when storing data on the chip.
    - if an employee's chip is compromised (eg cloned or the data from it skimmed by a malicious third party), company security may be at risk
    - encryption of the data on the chip and/or in the database
    - Security can be a range of similar and connected measures such as firewall, virus scanners, encryption, passwords

- limiting the amount of data stored on the chip/database to only the data needed to grant permissions – thus minimising the negative impact of any security breach
- implement two-factor authentication (eg the chip plus a PIN, app, text message or email passcode or extra biometric authentication (e.g. chip and eye scan))
- replace the chip with biometric authentication that has many of the benefits of the chip without the negatives of medical or ethical issues – evaluation needs to be a comparison with the chip otherwise it is a new technology description only and not applied to the problem of the chip technology
- the company would have to offer ongoing IT support to ensure that permissions were kept updated and data was reliable
    - company formulates a regular review/update strategy to ensure that data is kept current and accurate
- data about permissions (access to doors) is stored on the database, not on the RFID chip, so data can easily be updated
    - if the employee became the victim of fraud through the use of the chip, would the company be liable for the consequences?

Policy and procedural related solutions

- policies could be put in place (at a company or even a national level) to control the circumstances under which data could be collected, stored and used. These policies should be regularly reviewed/updated. Employees need to explicitly agree to those policies by giving their opt-in consent
- some employees may be particularly opposed/fearful about the implantation process or have cultural/religious objections to it
    - such employees could be allowed to wear the chip outside the body rather than have it implanted
- once implanted, the chip is always there and always “on”. Employees may have little control over how the data on the chip is used by the company and/or third parties
    - it might be possible for the employees to shield the chip (*eg* by wearing a specially designed glove or other shielded patch) to prevent it from being read outside situations chosen by them
    - a special glove can be worn to prevent unwanted/unknown/accidental access to information RFID implant
- the data on the chip may be compromised by a malicious third party
- encryption of the data on the chip and/or in the database
- limiting the amount of data stored on the chip/database to only the data needed to grant permissions – thus minimising the negative impact of any security breach.

If the evaluation does not provide any additional information to that in the article, the candidate will be awarded a maximum of ***[2]****.*

Marks	***Level descriptor***
0	*The response does not reach a standard described by the descriptors below.*
1–2	*One feasible solution to at least one problem is proposed and described. No evaluative comment is offered. Material is either copied directly from the article or implicit references are made to it.*
3–5	*One appropriate solution to at least one problem is proposed and partially evaluated. The response contains explicit references to information in the article that are partially developed. There is some use of appropriate ITGS terminology.*
6–8	*One appropriate solution to at least one problem is proposed and fully evaluated, addressing both its strengths and potential weaknesses. Areas for future development may also be identified. Explicit, fully developed references to the information in the article are made appropriately throughout the response. There is use of appropriate ITGS terminology.*