N16/3/ITGSX/BP2/ENG/TZ0/XX/M

Diploma Programme
Programme du diplôme
Programa del Diploma

Markscheme

November 2016

Information technology in a global society

Higher level and Standard level

Paper 2

14 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: Politics and government

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

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

Social/ethical concerns may include the following:

- surveillance – use of technology means that police are under constant surveillance from their superiors
- privacy – use of cameras on the devices, may mean that not just criminals are being watched. The everyday lives of police officers are being captured
- privacy – is the data related to personal details of victims and information about the crime stored securely in the central database
- privacy – known offenders because they were guilty of a crime and are in the area does not mean they are continuing in that criminal activity
- privacy – victims of crime – Neighbourhood Central
- reliability – over reliance on technology. Police may not be able to conduct their jobs effectively should technology fail
- reliability – Neighbourhood Central – citizens allowed to provide updates on known crime – potential for false, embellished information etc
- integrity of data – unauthorized changes to crime data could mean that crime data cannot be trusted
- security – accessing one central database on a variety of devices – could easily be hacked; loss of device
- security – use of third party apps for data storage and also the use of third party apps (Google Maps), both potentially have a security risk
- policies and standards – failure to have adequate policies in place on the use of devices could cause issues for the police department on how the mobile devices are used
- digital divide – impact on the job if police not familiar with using IT systems; impact on citizens who are not familiar with using the apps and do not know how to report updates and known crime, and to get alerts which reduces the effectiveness of the system.

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

Primary stakeholders may include the following:

- police officers – use app to gain information about crimes in an area or to report a crime
- citizens/witnesses – use the crime mapping tools to tip off the police with crime information, use it to see how safe their area is
- police department administrators – use the police app to determine where to locate the police officers
- criminals/known offenders – use the app to help decide where to commit the next crime
- App Developers – develop the police app and are responsible for fixing the bugs and testing the security of the data
- victims – whose details are logged on the smart device at the scene of the crime.

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: use of smartphones and tablets to report a crime or update information about a crime on the cloud server at London Police Headquarters.

Answers provided in the article include the following:

- Crime Report allows a police officer to report a crime
- digital maps provide crime information for a particular area
- clicking on each point allows a policeman to update information about a crime or enter details of a crime
- device cameras can be used to gather video evidence in real time
- creation of a single police database allows police officers to log in information
- authorizing the devices, this is part of setting up as is cross platform compatibility
- storage in 3rd party servers
- processing/data analysis by date, time, area, type – data visualize in range of graphs
- playback of videos and recordings
- sharing information by tags – send to colleague
- sharing of video.

Answers with additional information to that in the article may include the following:

Setting up:

- downloading the app
- registering with the police app including the username and password or personal information or mobile phone number for verification
- location services activated
- log on to police app
- the use of tools like apple configurator to “image” the device (more likely than download the app) including settings, security etc
- user name and password to log onto the TTS.

Input:

- input is via photo, voice, text, stylus, buttons on the device
- input uses touch screen, phone’s camera or microphone
- location services such as GPS are used to identify the area.

Connectivity:

- smart phone connects to wireless network or mobile broadband (via radio link) (3G, 4G, Wi-Fi)
- a client/server is used – phone is client, Police Headquarters provides cloud services
- data must be encrypted during transmission/decrypted at server.

Processing:
- app identifies police officers location via GPS or cell phone towers (triangulation) and identifies the police officer on the map
- view other reported crimes in the area
- select icons of crimes to read more information about the crimes
- if crime has already been reported – read information about the crime and take note of warning *eg* if criminal is dangerous. Click on the crime and key in additional information, police ID number and use camera to capture evidence – video/photo of the crime
- if crime is new, enter in required information in the compulsory fields *eg* select type of crime, details of crime, upload photo/video captured using smart phone or tablets
- each crime will be allocated a unique identifier so that this can be used to identify the crime and not mix up crime details of similar crimes in the same area
- crime details are submitted using submit button
- implication of real time streaming for video evidence
- use of queries and search criteria in analysing the data.

Storage:
- police database stores a new crime record using a unique identifier to identify the crime
- local storage of data for replay, editing or when connection is lost.

Output:
- confirmation message of crime reported is displayed on the screen with guidance on how to proceed with the crime (*eg* call for back up)
- auditory output – warning sounds
- output as graphs and visualization.

(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.

Answers may include the following:

Surveillance:
- built in location services could mean that police can be tracked while on duty (how); due to lack of policies (why).

Privacy:
- use of cameras on the devices, may mean that activities of citizens may be captured by police officers with no valid reason or whilst collecting evidence of a crime (how); Everyday lives of citizens may be captured and saved in the police database (how); photographs or videos captured in the call of duty may be taken from a distance, encompassing more than the crime but innocent bystanders (why). Tablet or phone cameras do not have sophisticated settings or zoom (why)
- Unauthorized access to data on crimes (how); due to lack of policies or security settings on the database could mean that video footage is accessed by others (why).
- privacy of known criminals, may mean people with a police record or who have formally committed crimes may be target or harassed (how); as the device identifies known offenders in the area (why)
- third party apps for storage or mapping data like google documents (how); may mean whoever has access can see potentially sensitive data (why).

Reliability:
- if technology fails, over reliance on technology could make it difficult for police officers to do their job:
  - *eg* phones lack of battery (how); phone apps *eg* video recorder use up battery quickly or older model phones have shorter battery life (why)
  - damage to phone when apprehending a criminal could mean that police may not have access to the crime data whilst doing their job which could put them in danger when approaching the scene of a crime (how); smart phone casing may not be that durable or could get wet or trodden on (why)
  - loss of Wi-Fi signal (how); as not all areas in a city have equal coverage. For example, this may include being blocked by a building or being underground (why)
  - maps may be out of date and updates may not reflect the current read layout, which may make location of crime scene inaccurate, send support to wrong location or misdirect officers (why).

Integrity of data:
- unauthorized edit or accidental edit of information by police officers (how); field properties not set correctly, or unauthorized access due to poor security settings on the phone, server, transmission could mean that data is not accurate (why)
- updating of known crimes by citizens (how); the updates may be false, mistaken, out of date or submitted in order to mislead the police (why).

Security:
- accessing one central database on a variety of devices – could easily be hacked by intercepting the data in transmission (how) – intercepting and decrypting of data in transmission due to lack of strong encryption (why)
- hacking the police database in the cloud (how); could be caused by breaches to firewall, lack of updating of server software (why)
- hacking into the phone/tablet (how) – security experts have to run security checks on all the different operating systems which could mean that some devices are less secure than others (as security loopholes are found by hackers all of the time), virus on the phone/tablet (why)
- security problems due to loss of device – phones/tablets can easily be lost when on duty (how); small devices could fall out of uniform pockets, easy pass codes and saved user details in the app could mean that criminals could gain access to the police database easily if found (why)
- control of access is not managed by the police but by the third party administrator (how); as data storage and google maps is administered by third party services.

Lack of policies and standards:
- failure to have adequate policies in place on the use of devices could cause issues for the police department on how the mobile devices are used by the police officer *eg* in breaching privacy of citizens, revealing too much sensitive information about police operations (how); police administrators may be unaware of the potential issues that could arise because they work in the office (why).

Candidates are expected to make reference to the 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 the 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.

Positive impacts to police officer may include the following:
- up to date information in real time – more prepared when approaching a crime – keep safer on the streets
- know where back up police are to help fight the crimes
- faster processing of crimes (less time not having to go back to the station)
- better crime statistics could lead to more promotions/pay increases/bonuses
- more job opportunities to develop the IT technology
- active involvement from community brings policing closer to community.

Negative impacts to police officer may include the following:
- over reliance of the app *eg* out of battery, no network coverage, slow to connect – may make their job difficult, more dangerous
- not all experienced police like new technology, they will need to be trained
- loss/damage of device may be costly if required to replace or repair
- if data has been tampered with, police may incorrectly report a crime or be misled into thinking that an area is safe
- surveillance – use of technology means that police are under constant surveillance from their superiors
- privacy – use of cameras on the devices, may mean that not just criminals are being watched. The everyday lives of police officers are being captured
- lack of policies and standards – can make the police officers job more difficult, *eg* information not being admissible in court; inappropriate actions by police officers provide loop holes for criminals.

Positive impacts to the citizen/witness/victim may include the following:
- safer streets – minor criminals may be deterred. Police are more equipped to solve crimes
- more evidence collected for court cases – which may mean more successful prosecutions
- can make valued decision about moving to a certain area.

Negative impacts to the citizen/witness/victim may include the following:
- innocent citizens may have privacy invaded due to the increase in surveillance using the police devices
- citizens living in areas of poor Wi-Fi or mobile network coverage may not be as protected
- value of house prices may fall in areas where the trend of increased crimes is detected and shared with the public
- if criminals are able to intercept the crime database and use this data, the areas could become less safe
- unauthorized access to crime data that is then shared with the public, could expose citizens who were falsely linked to a crime
- integrity of data – unauthorized changes to crime data could mean that crime data cannot be trusted and innocent citizens may be accused of crimes
- lack of policies by the police department could lead to misuse which could negatively affect citizens
- third party server maintained by third party so may be difficult to find out who else has access to data apart from police officials.

Positive impacts to the police department/administrators, app developers may include the following:

- easier supervision of police officers (as can track them)
- save on manpower as police officers can be more efficient
- reduced costs due to less police required to do the same job
- improved employment opportunities
- increased efficiency in terms of time, cost and effort
- increased effectiveness in terms of improved accuracy of data collected, and presentation to various stakeholders
- third party support so there is no need to invest in cloud technology/cost savings.

Negative impacts to the police department may include the following:

- increased costs at providing the IT solution – devices, development of apps
- harder for the technical department to support and manage a multi-platform solution, there may be more security issues to deal with
- good experienced police officers may not be as efficient as they should be due to lack of technical expertise
- the need for training and costs involved
- many police officers may find it difficult/inconvenient to use technology
- if data is breached at third party end, police will lose face
- technology failure may lead to disruption and huge backlog, over reliance on technology and loss of intuition
- device theft/loss can lead to misuse if in wrong hands
- job losses as less police are needed to carry out the policing but more to maintain the technology.

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**.

Answers may include the following:

Solutions to problems of surveillance:
- policies on who has access to the information on the location of police officers and their movements and how this information is used
- police officers can turn off GPS tracking/location services at will.

Solutions to problems of security/privacy/integrity of data:
- crime data is encrypted during transmission and on the central server in the cloud
- restricted access to information stored on central server of the online store, *ie* employees can only view necessary information
- authentication for employees of police who have permission to access the database
- policies can be established
- audit trails/logs kept to show who accesses data and when
- authentication methods such as strong password/biometric/MAC address/IP address used during log in
- security training for employees
- data on the server not shared with other parties/kept on server in police offices.

Solutions to the problem of reliability of the cloud server:
- redundancy is built in to the system – a backup server is in place in case the main server crashes (this is part of the cloud service providers now but needs to be explained that there have been occasions when these large backup systems have not worked)
- police department policies – include procedures/alternative uploading schedule to address technical problems
- police department policies – to handle unforeseen problems, for example police officers who have not made backups or cannot send data due to technical problems.

Solutions to the problem of the reliability of the police devices and access to the cloud server:
- availability of other devices *eg* spare device in the police car
- other ways of accessing the public network to access the police server (Wi-Fi hotspots)
- temporary storing the crime on the device until a network is established
- device tracking software activated in case of lost phone – software that allows the device to be locked, wiped, located on a map or even see the face of the user with the device camera
- police department policies for loss/theft/damaged devices – include procedures and how to address the technical problems.

Solutions to the problem of lack of policies on appropriate use of the technology:
- policies need to be developed which include the what, the how, the where, the when technology should be used. This should be developed by police administrators and shared with all departments of the police across the country.

*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.