Candidate surname	Other names
Centre Number	**Learner Registration Number**

Level 3 Alternative Academic Qualification BTEC National (Extended Certificate)

Practice Examination Paper

Time: 2 hours 15 minutes	RTH-60298T

Information Technology

UNIT 2: Cyber Security and Incident Management

You do not need any other materials.	Total Marks

Instructions

- Use black ink or ball-point pen.
- Fill in the boxes at the top of this page with your name, centre number and learner registration number.
- Answer **all** questions.
- Answer the questions in the spaces provided – *there may be more space than you need*.

Information

- The total mark for this paper is **90**.
- The marks for **each** question are shown in brackets – *use this as a guide as to how much time to spend on each question*.

Advice

- Read each question carefully before you start to answer it.
- Try to answer every question.
- Check your answers if you have time at the end.

Answer ALL questions. Write your answers in the spaces provided.

Rons Tech Hub (RTH) is an independent electronics retail and repair business with several high-street branches across the UK, managed by its founder, Ron.

Each branch operates a repair workshop where technicians use diagnostic workstations connected via wired Ethernet to a local branch server. Each branch also provides a separate wireless network so customers can connect their personal devices while waiting in the reception area.

All RTH branches are supported remotely by a central IT administration team based at the head office.

Figure 1 shows an incomplete network diagram for one RTH branch.

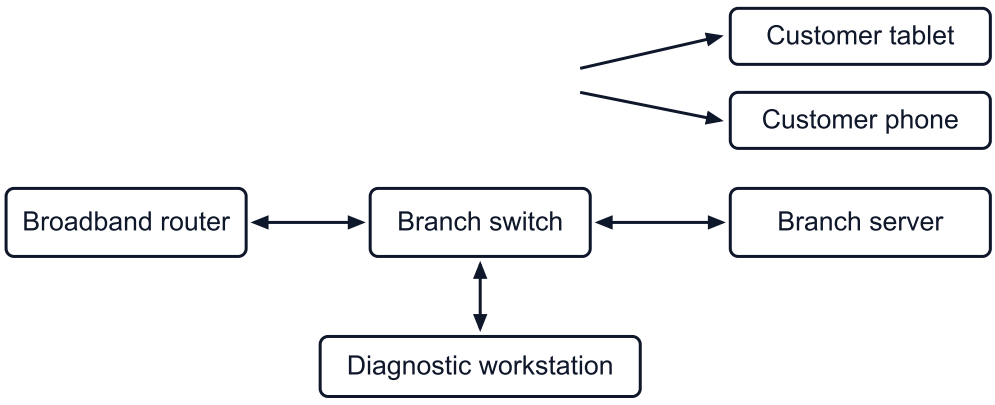

Figure 1

(e) Explain why a rootkit is difficult to detect by standard antivirus software. **(2)**

Careless handling of hardware by workshop staff could cause accidental damage to RTH's digital systems.

(b) Name two other causes of accidental or environmental damage to computer systems. **(2)**

1

2

One possible impact of a cyber attack is reputational loss.

(c) Name two other possible impacts a cyber attack could have on RTH. **(2)**

1

2

A workstation in Ron's branch has been infected with ransomware (an encryptor).

(d) Explain how the ransomware infection will affect the technicians' ability to use the workstation. **(2)**

(e) Explain why a rootkit is difficult to detect by standard anti-virus software. **(2)**

(f) Explain one way that poor security culture among staff can lead to accidental disclosure of sensitive customer data. **(2)**

(g) Explain how an unauthorised person could gain physical access to an unattended workstation in the reception area to steal data. **(2)**

Currently, all workshop technicians use a shared single-factor PIN to access the secure parts storeroom. Ron is considering replacing this with biometric scanners that use iris recognition or retinal scanning.

(e) Evaluate the security implications of replacing the PIN system with biometric iris recognition or retinal scanning. **(9)**

(Total for Question 1 = 23 marks)

2 Ron plans to upgrade the network infrastructure and security across all RTH branches.

Each branch connects to the head office over a Wide Area Network (WAN).

(a) Name one type of private network that RTH could use to share internal resources with staff or external suppliers. **(1)**

Before launching the upgraded system, RTH wants to check for security weaknesses.

(b) Name two types of tool or method that can be used to assess vulnerabilities in RTH's computer systems. **(2)**

1

2

(c) Explain the function of a firewall in protecting the branch network. **(2)**

Old solid-state drives (SSDs) and magnetic backup tapes containing customer repair histories are being retired.

(d) Explain two different methods of securely disposing of these storage media. **(4)**

1

2

Ron wants branch managers to use certificate-based authentication or hardware security tokens when logging into head office systems.

(e) Describe how a hardware security token authenticates a user. **(2)**

(f) Explain why RTH should configure automatic screen locks after failed login attempts on branch workstations. **(2)**

Ron is considering moving RTH's customer repair booking database and invoices to a cloud computing platform.

(g) Evaluate the security implications of using cloud computing to store and manage customer data across all RTH branches. **(9)**

(Total for Question 2 = 22 marks)

3 RTH technicians use handheld diagnostic tablets that connect wirelessly to test equipment and the branch network.

One type of wireless connection used is Bluetooth.

(a) Name two other types of wireless connection. **(2)**

1

2

Network traffic between the branch and head office uses the Transmission Control Protocol/Internet Protocol (TCP/IP) suite and Network Address Translation (NAT).

(b) Explain two differences between TCP and User Datagram Protocol (UDP) packets. **(4)**

1

2

Ron is concerned that attackers sitting outside the shop could target the branch's Wireless Local Area Network (WLAN).

(c) Explain two precautions RTH can take to protect its internal WLAN from unauthorised access. **(4)**

1

2

All RTH staff must follow a strict password management policy when creating and storing their login credentials.

(d) Explain two password management practices that help keep staff accounts secure. **(4)**

1

2

Currently, all workshop technicians use a shared single-factor PIN to access the secure parts storeroom. Ron is considering replacing this with iris/retina biometric scanners.

(e) Evaluate the security implications of replacing the PIN system with biometric iris/retina recognition. **(9)**

(Total for Question 3 = 23 marks)

4 A technician's branch desktop computer has been compromised by an external hacker, resulting in customer personal details being copied and leaked online.

(a) Name two types of financial loss RTH could experience as a result of this data breach. **(2)**

1

2

(b) Explain one piece of UK legislation that relates to RTH's duty to protect customer personal data. **(2)**

An external digital forensics investigator is called in to examine the compromised desktop computer and network.

(c) Explain two actions the investigator should take to maintain the reliability and admissibility of forensic evidence. **(4)**

1

2

(d) Explain why the investigator would perform network forensics on the branch's router and firewall logs. **(3)**

During the investigation, technicians want to verify that a downloaded software patch has not been altered before installing it on clean machines.

(e) Explain how a checksum or file integrity check verifies that a file has not been tampered with. **(2)**

Following the attack, Ron asks the central IT administration team to introduce a formal cyber security incident response policy across all RTH branches.

(f) Evaluate the benefits and drawbacks of having a formal cyber security incident response policy in place at RTH. **(9)**

(Total for Question 4 = 22 marks)

TOTAL FOR PAPER = 90 MARKS

Mark Scheme (Practice Assessment)

Level 3 AAQ BTEC National (Extended Certificate) in Information Technology
Unit 2: Cyber Security and Incident Management (Paper Ref: RTH-60298T)

Rons Tech Hub

General Marking Guidance

- All candidates must receive the same treatment. Examiners must mark the first candidate in exactly the same way as they mark the last.
- Mark schemes should be applied positively. Candidates must be rewarded for what they have shown they can do rather than penalised for omissions.
- There is no ceiling on achievement. All marks on the mark scheme should be used appropriately.
- All the marks on the mark scheme are designed to be awarded. Examiners should always award full marks if deserved, i.e. if the answer matches the mark scheme or provides an alternative technically valid response using different wording. Examiners should also be prepared to award zero marks if the candidate's response is not worthy of credit according to the mark scheme.
- Indicative content lists are non-prescriptive examples rather than exhaustive lists of all acceptable answers. Where some judgement is required, mark schemes will provide the principles by which marks will be awarded and exemplification may be limited.
- Do not award multiple marks for essentially the same point unless the candidate has developed or expanded the explanation as required by the marking criteria.
- Crossed out work should be marked UNLESS the candidate has replaced it with an alternative response.

Question 1 (Total: 23 marks)

Question	Answer	Mark
1 (a)	**Spec Ref: B1.1.4 / B2.1.2** Award one mark for adding and labelling an appropriate wireless device (e.g. Wireless Access Point / WAP / Wi-Fi access point / wireless router). Award one mark for drawing a valid connection line linking the added device to the **Branch switch** (and meeting the existing customer device arrows). *Note: Shape of the drawn symbol is irrelevant. Do not award the connection mark if connected directly to the Branch server or Diagnostic workstation.*	**(2)**

Question	Answer	Mark
1 (b)	**Spec Ref: A1.1.2** Award one mark for each valid cause up to a maximum of two marks: • Fire • Flood / water spillage / liquid damage • Power loss / power surge • Natural disaster (accept once only in place of fire/flood/etc.) *Accept any other appropriate response. Do not accept data leaks or cyber attacks.*	**(2)**
1 (c)	**Spec Ref: A1.3** Award one mark for each valid impact up to a maximum of two marks: • Operational loss • Financial loss • Intellectual property (IP) loss *Accept specific examples of these categories (e.g. loss of trade secrets, regulatory fines, loss of service availability). Do not accept examples of reputational loss.*	**(2)**
1 (d)	**Spec Ref: A1.2.1** Award one mark for identifying an effect, and one mark for an appropriate linked expansion, up to a maximum of two marks: • Files/data on the workstation will be encrypted (1), preventing technicians from opening customer records or diagnostic tools until the files are recovered, for example, from a backup (1). • A ransom demand screen/message locks the interface (1), stopping technicians from accessing the operating system or performing repairs (1). *Accept any other appropriate technically valid response. Do not imply that paying a ransom guarantees recovery.*	**(2)**
1 (e)	**Spec Ref: A1.2.1 / A4.1.3** Award one mark for identifying a characteristic, and one mark for an appropriate linked expansion, up to a maximum of two marks: • It can operate at a privileged level of the operating system, such as the kernel or boot level (1), allowing it to hide its files and processes from standard antivirus scans (1). • It can intercept/modify operating system calls (1) so that requests to inspect infected files return clean/altered results to the antivirus software (1). *Accept any other appropriate wording or technically valid explanation.*	**(2)**

Question	Answer	Mark
1 (f)	**Spec Ref: A1.1.4** Award one mark for identifying a reason, and one mark for an appropriate linked expansion, up to a maximum of two marks: • Staff treat security rules casually/ignore procedures (1) such as emailing unencrypted customer repair spreadsheets to the wrong recipient (1). • Staff share login passwords or write them down on sticky notes (1) allowing unauthorised visitors/colleagues to view confidential customer records (1). • Lack of staff awareness/training on data handling (1) leading to staff leaving printed invoices or customer screens visible in public areas (1). *Accept any other appropriate response.*	**(2)**
1 (g)	**Spec Ref: A1.2.5** Award one mark for identifying a method, and one mark for an appropriate linked expansion, up to a maximum of two marks: • Walking up to an unlocked reception computer while staff are distracted (1) and copying files onto a USB flash drive / emailing files out (1). • Shoulder surfing a staff member typing their PIN/password (1) and then logging into the unattended workstation when the staff member steps away (1). *Accept any other appropriate response focused on accessing an unattended device.*	**(2)**

Question	Answer	Mark
1 (h)	**Spec Ref: A1.2.4** Responses will be credited according to the candidate's demonstration of knowledge and understanding of the material, using the indicative content and level descriptors below. **Indicative content (non-prescriptive — credit other valid contextual points):** • **Pretexting / Impersonation:** Attackers could phone a branch pretending to be from RTH's central IT administration team, creating a false sense of urgency (e.g. an urgent server patch) to trick technicians into revealing admin passwords or installing remote access software. • **Spear Phishing:** Targeted emails crafted using publicly available details about Ron or specific branch managers, making malicious links or invoice attachments appear genuine and harder to spot than generic phishing. • **Generic Phishing / Vishing / Smishing:** High-volume fake supplier invoices or courier delivery texts sent to busy reception desks; easier to identify due to generic greetings or poor grammar, though busy retail environments increase the risk of human error. • **Mitigating Factors & Counterarguments:** Threat can be reduced through regular staff security awareness training, strict verification protocols before sharing credentials with head office IT, multi-factor authentication (MFA), and email spam/phishing filters. • **Conclusion:** A reasoned judgement weighing the high vulnerability of busy customer-facing retail/repair staff against the effectiveness of RTH's technical controls and staff training.	**(9)**

Level	Mark	Descriptor (Applies to Questions 1(h), 2(g), 3(e) and 4(f))
Level 0	0	No rewardable material.
Level 1	1–3	• Demonstrates basic application of knowledge and understanding that is partially relevant to the context of the question and may consider only one side of the context (AO2). • Demonstrates a basic analysis of the situation by superficially breaking down the different aspects into their component parts (AO3 – Analysis). • Demonstrates a basic evaluation which partially considers different factors/events and competing points, leading to a conclusion which is superficial or unsupported (AO3 – Evaluation).
Level 2	4–6	• Demonstrates good application of knowledge and understanding that is relevant to the context of the question and considers both sides of the context (AO2). • Demonstrates a good analysis of the situation by breaking down the different aspects into their component parts (AO3 – Analysis). • Demonstrates a good evaluation which considers different factors/events and competing points, leading to a conclusion which is partially supported (AO3 – Evaluation).

Level	Mark	Descriptor (Applies to Questions 1(h), 2(g), 3(e) and 4(f))
Level 3	7–9	• Demonstrates comprehensive application of knowledge and understanding that is consistently relevant to the context of the question and considers both sides of the context in a balanced way (AO2). • Demonstrates a thorough analysis of the situation by comprehensively breaking down the different aspects into their component parts (AO3 – Analysis). • Demonstrates a thorough evaluation which comprehensively considers different factors/events and competing points, leading to a conclusion which is well supported (AO3 – Evaluation).

Question 2 (Total: 22 marks)

Question	Answer	Mark
2 (a)	**Spec Ref: B1.1.2** Award one mark for one of the following: • Intranet • Extranet • Cloud network *Accept Virtual Private Network (VPN). Do not accept LAN or WAN.*	**(1)**
2 (b)	**Spec Ref: A2.4 / A2.6** Award one mark for each valid tool or method up to a maximum of two marks: • Port scanner • Network mapper / system discovery tool • Registry checker • Website vulnerability scanner • Vulnerability detection and management software • Penetration testing *Accept any other appropriate vulnerability assessment tool or method. Do not accept protective controls such as firewalls or antivirus software.*	**(2)**
2 (c)	**Spec Ref: A4.1.4 / B3.3.5** Award one mark for identifying a function, and one mark for an appropriate linked expansion, up to a maximum of two marks: • It monitors and filters incoming and outgoing network traffic (1) blocking unauthorised packets based on predefined security rules/ports/IP addresses (1). • It acts as a barrier between the internal branch network and external networks/internet (1) preventing malicious traffic from reaching branch servers/workstations (1). *Accept any other appropriate response.*	**(2)**

Question	Answer	Mark
2 (d)	**Spec Ref: B2.2.2** Award one mark for identifying a disposal method, and one mark for an appropriate linked expansion, up to a maximum of four marks (two distinct methods × 2 marks): • Secure erasure/sanitisation (1) using an appropriate manufacturer-supported SSD secure erase or sanitisation method to remove stored data (1). • Cryptographic erasure (1) by securely destroying the encryption key used to protect the data, where the SSD was encrypted (1). • Physical destruction (1), such as using an approved specialist shredding or crushing process to destroy the SSD chips or magnetic tape (1). • Degaussing — *applicable to magnetic backup tapes only* (1) using a strong magnetic field to erase/reset the magnetic patterns storing the data (1). *Accept any other appropriate technically valid response. Note: Degaussing is only valid for magnetic storage media (tapes), not SSDs.*	**(4)**
2 (e)	**Spec Ref: A4.1.5** Award one mark for each appropriate point in a linked description up to a maximum of two marks: • The user connects/inserts a physical USB key or smartcard into the computer (1) which verifies possession of the device alongside their login credentials (1). • A disconnected token generates a one-time code independently (1) which the manager must type into the login prompt to prove their identity (1). *Accept contactless Bluetooth/Near-field communication (NFC) dongles or any other appropriate wording.*	**(2)**
2 (f)	**Spec Ref: A4.1.9** Award one mark for identifying the mechanism, and one mark for an appropriate linked expansion, up to a maximum of two marks: • It automatically disables/locks the login screen after a set number of incorrect password entries (1) preventing attackers from using brute-force/guessing attacks to gain access (1). *Accept any other appropriate wording.*	**(2)**

Question	Answer	Mark
2 (g)	**Spec Ref: A2.1.8 / B1.4.2** Use the Level Descriptors table above (0–9 marks). **Indicative content (non-prescriptive):** • **Security Risks / Drawbacks:** Customer PII and invoice data must travel over the internet between branches and the cloud, creating risks of interception/tampering if encryption (TLS/VPN) is weak; reliance on third-party provider security and potential insider access by cloud vendor staff; risk of misconfigured default cloud access settings or insecure APIs exposing data across branches; loss of access to booking records if branch internet connectivity drops. • **Security Benefits / Advantages:** Reputable cloud providers employ dedicated security specialists, enterprise firewalls, and automated patching/updates that exceed what an independent retail business could maintain locally; built-in automated backups and multi-site redundancy improve data resilience against local branch hardware failure, fire, or theft. • **Conclusion:** A balanced judgement weighing RTH's reduced local maintenance burden and stronger provider-managed resilience against the loss of direct control and reliance on secure internet connectivity.	(9)

Question 3 (Total: 23 marks)

Question	Answer	Mark
3 (a)	**Spec Ref: A2.3.1 / B2.1.3** Award one mark for each valid wireless connection type up to a maximum of two marks: • Wi-Fi (IEEE 802.11) • Near-field communication (NFC) • Radio-frequency identification (RFID) • Cellular / mobile data (3G, 4G, 5G) • Infrared (IR) • Li-Fi • Satellite link • Zigbee *Accept any other valid wireless connection technology. Do not accept "Bluetooth", "radio", or "tethering".*	(2)

Question	Answer	Mark
3 (b)	**Spec Ref: B3.1.1 / B3.1.3** Award one mark for identifying a difference, and one mark for an appropriate linked explanation, up to a maximum of four marks (two differences × 2 marks): • TCP is connection-oriented / establishes a handshake before sending (1) whereas UDP is connectionless and sends packets immediately without establishing a session (1). • TCP provides error checking/correction and retransmits lost packets (1) whereas UDP does not guarantee delivery or retransmit dropped packets (1). • TCP sequences packets so they arrive in the correct order (1) whereas UDP packets may arrive out of order with lower overhead/faster speed (1). *Accept any other appropriate technical comparison.*	**(4)**
3 (c)	**Spec Ref: A4.3** Award one mark for identifying a precaution, and one mark for an appropriate linked explanation, up to a maximum of four marks (two distinct precautions × 2 marks): • Use strong wireless encryption such as WPA2 or WPA3 (1) so intercepted wireless packets cannot be read by outsiders without the encryption key (1). • Implement MAC address filtering / allow lists (1) so only registered RTH diagnostic tablets with approved hardware addresses can connect to the access point (1). • Hide the Service Set Identifier (SSID) broadcast (1), reducing the visibility of the network to casual users scanning for available Wi-Fi networks, although this should not be relied upon as the only security measure (1). • Change default administrator passwords and router settings (1) preventing attackers from logging into the access point using known factory credentials (1). • Disable Wi-Fi Protected Setup (WPS) (1) to prevent attackers exploiting known PIN vulnerabilities to gain access (1). *Accept any other appropriate technically valid response.*	**(4)**

Question	Answer	Mark
3 (d)	**Spec Ref: A2.1.2 / C1.1.1** Award one mark for identifying a practice, and one mark for an appropriate linked explanation, up to a maximum of four marks (two practices × 2 marks): • Using a dedicated/encrypted password manager (1) to generate and securely store unique, complex passwords for every system without staff writing them down (1). • Enforcing a minimum password age / restricting password reuse (1) so staff cannot immediately revert back to an old password or recycle compromised credentials (1). • Prohibiting password sharing / multiple simultaneous logons with the same account (1) ensuring individual accountability and preventing unauthorised access if one user's details leak (1). • Disabling browser auto-fill on shared workstations (1) so subsequent users of the machine cannot automatically log into another technician's account (1). *Accept any other appropriate response.*	**(4)**
3 (e)	**Spec Ref: A4.1.5 – User Authentication** Use the Level Descriptors table above (0–9 marks). **Indicative content (non-prescriptive — credit other valid contextual points):** • **Security Advantages:** Eliminates the risk of a shared PIN being overheard, shoulder-surfed, or shared with unauthorised individuals; iris or retinal patterns provide a distinctive biometric identifier, making it difficult for an unauthorised person to impersonate a technician when appropriate security and detection measures are used; provides accurate audit trails showing exactly which technician entered the storeroom and when; staff cannot forget or lose their biometric trait. • **Security & Operational Drawbacks:** High initial hardware and installation cost across multiple RTH branches; if stored biometric templates are compromised in a breach, a user's iris or retinal characteristics cannot be reset or reissued like a PIN; false rejections may occur due to lighting glare, glasses/contact lenses, or eye irritation/dust in a repair workshop, slowing down technicians; privacy/GDPR concerns around storing sensitive biometric data. • **Conclusion:** A reasoned judgement comparing the major security upgrade over a weak shared PIN against the high cost, workshop usability issues, and the long-term consequences of biometric data being compromised, as biometric characteristics cannot simply be changed like a PIN or password.	**(9)**

Question 4 (Total: 22 marks)

Question	Answer	Mark
4 (a)	**Spec Ref: A1.3.2** Award one mark for each valid type of financial loss up to a maximum of two marks: • Regulatory fines / penalty payments (e.g. ICO fines under UK GDPR) • Compensation payments / refunds to affected customers • Legal fees / statutory investigation costs • Loss of profits / cash flow problems • Increased cyber insurance premiums/costs • Costs of remedial actions (e.g. paying for identity/credit monitoring for customers) *Accept any other appropriate financial loss. Do not accept operational or reputational loss unless explicitly linked to a financial cost.*	**(2)**
4 (b)	**Spec Ref: A3.1.1 / A3.3.1** Award one mark for identifying the legislation, and one mark for an appropriate linked explanation, up to a maximum of two marks: • General Data Protection Regulation (UK GDPR) / Data Protection Act 2018 (1) which requires organisations to implement appropriate technical and organisational measures to maintain the confidentiality and integrity of personal data (1). *Accept any other appropriate wording.*	**(2)**
4 (c)	**Spec Ref: D2.1.1 / D2.1.2 / D2.1.3** Award one mark for identifying an action, and one mark for an appropriate linked explanation, up to a maximum of four marks (two distinct actions × 2 marks): • Work on a forensic copy/bit-stream image rather than the original hard drive (1) to prevent altering or corrupting original evidence on the suspect machine (1). • Maintain a strict chain of custody record (1) documenting everyone who handled, accessed, or transferred the device so evidence cannot be challenged as tampered with in court (1). • Calculate a cryptographic hash value for the original drive and the forensic image (1), then compare the values to check that the image matches the original and has not been altered (1) *(also credit explaining that the hash value can be calculated again later to verify the forensic image has remained unchanged, providing strong evidence of integrity)*. • Keep contemporaneous notes/logs of all investigative actions taken (1) recording any intentional or unintentional alterations made during analysis (1). *Accept any other appropriate technically valid response.*	**(4)**

Question	Answer	Mark
4 (d)	**Spec Ref: D1.1.3 / D2.2.2** Award one mark for identifying a reason, one mark for an appropriate linked explanation, and a further mark for a linked expansion up to a maximum of three marks: • To trace unusual inbound or outbound network traffic (1), identifying suspicious source IP addresses or unusual geographical locations (1), helping investigators understand where the suspicious activity may have originated and whether data could have been exfiltrated (1). • To detect unusual port usage or unauthorised connections (1) showing whether an attacker moved laterally to other branch devices (1) so RTH knows the full scope of the compromise (1). *Accept any other appropriate technically valid response.*	**(3)**
4 (e)	**Spec Ref: A4.1.3 / D2.1.1** Award one mark for identifying how a checksum works, and one mark for an appropriate linked explanation, up to a maximum of two marks: • A cryptographic hashing algorithm calculates a fixed-length hash value from the downloaded file's contents (1). This value is compared with the trusted hash supplied by the publisher; if the values differ, this indicates that the file has been changed or corrupted (1). *Accept any other appropriate wording that accurately explains hash comparison without claiming mathematical uniqueness.*	**(2)**
4 (f)	**Spec Ref: C1.1.5** Use the Level Descriptors table above (0–9 marks). **Indicative content (non-prescriptive — credit other valid contextual points):** • **Benefits:** Provides clear step-by-step checklists and escalation flowcharts so branch staff know immediately how to contain an attack (e.g. isolating infected machines) without panicking; defines clear roles and emergency contacts (head office IT, legal, ICO, PR, insurance) reducing response delays and financial/reputational damage; ensures forensic evidence and contemporaneous notes are preserved properly from the start; supports the organisation in demonstrating accountability and preparedness under UK GDPR when the policy is properly implemented, maintained and reviewed. • **Drawbacks:** Developing, maintaining, and regularly testing the policy across multiple branches requires significant time and management resources; staff may fail to follow procedures during a stressful live incident if they have not received regular practical training or if they fear blame for reporting mistakes; an overly rigid policy may struggle to cover novel or unforeseen attack scenarios. • **Conclusion:** A balanced judgement concluding that a formal incident response policy is essential for coordinating RTH's multi-branch response and limiting breach damage, provided it is backed by ongoing staff training and regular drills.	**(9)**