Higher National Unit Specification

General information

Unit title: Mobile Device Management (MDM) and Mobile Application Management (MAM): Introduction (SCQF level 8)

Unit code: HT9M 35

Superclass: CB

Publication date: August 2017

Source: Scottish Qualifications Authority

Version: 01

Unit purpose

The purpose of this unit is to introduce learners to a range of Mobile Device Management (MDM) and Mobile Application Management (MAM) technologies that enable secure smartphone and tablet use in businesses and organisations. It is a specialist unit, intended for learners undertaking a Higher National qualification in a Computing related area.

The unit covers the factors involved in maintaining the reliability and security of data and devices in a Mobile Device Management (MDM) and Mobile Application Management (MAM) system. The unit also covers the key features of a Mobile Device Management solution. The unit explores the key features of a Mobile Application Management solution such as distributing, securing, and tracking the organisation's mobile applications. Learners should be able to use and configure different functionalities of a MAM system. The unit also covers the security issues and solutions provided by Mobile Device Management and Mobile Application Management systems. Learners will explore different threats and vulnerabilities that affect mobile devices and will investigate effective mobile security solutions.

On completion of this unit, learners will understand the principal features of a Mobile Device Management and Mobile Application Management system, the security threats that exist and the solutions provided by MDM and MAM systems. They will be able to implement basic configuration of a MDM/MAM system.

Higher National Unit Specification: General information (cont)

Unit title: Mobile Device Management (MDM) and Mobile Application Management (MAM): Introduction (SCQF level 8)

Outcomes

On successful completion of the unit the learner will be able to:

1 Describe factors involved in maintaining the reliability and security of data and devices in a Mobile Device Management and Mobile Application Management system.
2 Evaluate key features of a Mobile Device Management system.
3 Evaluate key features of a Mobile Application Management system.
4 Describe security issues and solutions provided by Mobile Device Management (MDM) and Mobile Application Management (MAM) systems.
5 Implement basic configuration of a MDM/MAM system.

Credit points and level

1 Higher National Unit credit at SCQF level 8: (8 SCQF credit points at SCQF level 8)

Recommended entry to the unit

Learners should possess basic IT skills before commencing this unit. This may be evidenced by possession of the Core Skill in *Information and Communication Technology* at SCQF level 5 (or equivalent).

Core Skills

Opportunities to develop aspects of Core Skills are highlighted in the support notes for this unit specification.

There is no automatic certification of Core Skills or Core Skill components in this unit.

Context for delivery

If this unit is delivered as part of a group award, it is recommended that it should be taught and assessed within the subject area of the group award to which it contributes.

Equality and inclusion

This unit specification has been designed to ensure that there are no unnecessary barriers to learning or assessment. The individual needs of learners should be taken into account when planning learning experiences, selecting assessment methods or considering alternative evidence.

Further advice can be found on our website **www.sqa.org.uk/assessmentarrangements**.

Higher National Unit Specification: Statement of standards

Unit title: Mobile Device Management (MDM) and Mobile Application Management (MAM): Introduction (SCQF level 8)

Acceptable performance in this unit will be the satisfactory achievement of the standards set out in this part of the unit specification. All sections of the statement of standards are mandatory and cannot be altered without reference to SQA.

Where evidence for outcomes is assessed on a sample basis, the whole of the content listed in the knowledge and/or skills section must be taught and available for assessment. Learners should not know in advance the items on which they will be assessed and different items should be sampled on each assessment occasion.

Outcome 1

Describe factors involved in maintaining the reliability and security of data and devices in a Mobile Device Management and Mobile Application Management system.

Knowledge and/or skills

- Types of mobile devices
- Types of mobile operating systems
- Types of networks utilised by mobile devices
- Types of MDM/MAM systems
- Data transfer from the mobile device and application to the enterprise server
- Data protection on the device and storage, in transit and if lost/stolen
- Centralised control over all mobile devices, data, and applications
- Mobile Device Management/Mobile Application Management architecture

Outcome 2

Evaluate key features of a Mobile Device Management system.

Knowledge and/or skills

- Cross-platform device support
- Configuration management
- Device monitoring
- Licence control
- Software distribution
- Inventory and asset control
- Remote control
- Connection management
- Scheduling and prioritisation
- Process automation
- Document and content distribution
- Bandwidth optimisation

Higher National Unit Specification: Statement of standards (cont)

Unit title: Mobile Device Management (MDM) and Mobile Application Management (MAM): Introduction (SCQF level 8)

Outcome 3

Evaluate key features of a Mobile Application Management system.

Knowledge and/or skills

- Distribution of mobile applications
- Security of mobile applications
- Tracking mobile applications

Outcome 4

Describe security issues and solutions provided by Mobile Device Management (MDM) and Mobile Application Management (MAM) systems.

Knowledge and/or skills

- Threats and vulnerabilities that affect mobile devices and applications
- Effective mobile security solutions

Outcome 5

Implement basic configuration of a MDM/MAM system.

Knowledge and/or skills

- Remote management of applications
- Automatic installation of applications during enrolment
- On-demand installation of applications from the enterprise app catalogue
- Access configuration of application on assignment rules
- Restriction of application usage by creating blacklists, whitelists, and application compliance policies
- Restriction of access to pre-installed applications on a device
- Disabling application stores
- Prevention of data backup and automatically remove applications
- Tracking and viewing installed, approved, and blacklisted applications at the device and user level
- Configuration of alerts when an end user has installed an unapproved application
- Generating application inventory, version history, and compliance reports

Higher National Unit Specification: Statement of standards (cont)

Unit title: Mobile Device Management (MDM) and Mobile Application Management (MAM): Introduction (SCQF level 8)

Evidence requirements for this unit

Learners will need to provide evidence to demonstrate their knowledge and/or skills across all outcomes by showing that they can produce:

1 knowledge evidence (for Outcomes 1, 2, 3 and 4).
2 product evidence (for Outcome 5).

The knowledge evidence will be the definitions, descriptions, explanations and evaluations required for Outcomes 1, 2, 3 and 4. Evidence is normally required for all of the associated knowledge; however, sampling is permissible in certain circumstances (see below). However, it is important that no key piece of knowledge is omitted. This evidence may be produced over the life of the unit, under loosely controlled conditions (including access to reference materials). Authentication will be necessary (see below).

The knowledge evidence may be sampled when testing is used. When testing is used, it must be under supervised conditions and controlled in terms of location, timing and access to reference materials.

The product evidence required for Outcome 5 will be the configuration of a MDM/MAM solution which must be described or recorded such as screen shots or screen recordings.

When evidence is produced in uncontrolled or loosely controlled conditions it must be authenticated. *The Guide to Assessment* provides further advice on methods of authentication.

Higher National Unit support notes

Unit title: Mobile Device Management (MDM) and Mobile Application Management (MAM): Introduction (SCQF level 8)

Unit support notes are offered as guidance and are not mandatory.

While the exact time allocated to this unit is at the discretion of the centre, the notional design length is 40 hours.

Guidance on the content and context for this unit

This unit has been designed to offer learners an introduction to Mobile Device Management and Mobile Application Management technologies that enable secure smartphone and tablet use in business and organisations. The main focus of the unit should be on the implementation and configuration of Mobile Device Management and Mobile Application Management systems. The intention of this unit is to keep the outcomes as generic as possible, leaving it up to each centre as to which tools and devices to opt for.

One of the main aims of the unit is for learners to give consideration to the challenges that organisations are forced to face when integrating mobile devices in their existing information and communication infrastructures. It should be stressed to the learner that the entrance of mobile devices in business environments enhances productivity and business process optimisations, however this also raises a lot of possible vulnerabilities and security leaks. Discussions should explore different threats and vulnerabilities that affect mobile devices which include: loss of phones and other mobile devices, theft of private information if the mobile device is lost or stolen, annoying, unwanted calls and text messages, mobile viruses, malware and other threats, cybercriminals, dangerous websites, harmful downloads, infected SD memory cards. Emphasis should be made on effective mobile security solutions such as password protection, on-device data encryption, data-fading, over the air data encryption, patch management.

When exploring factors involved in maintaining the reliability and security of data and devices in a MDM and MAM system, learners should investigate typical mobile devices that have second generation enterprise mobility capabilities and are used in the business environment. Learners should be encouraged to compare features of different types of mobile devices and mobile operating systems. The discussion around the types of networking such as WPAN, WLAN, WWAN, or satellite should highlight how these influence the amount of data transferred from the mobile application to the enterprise server. Learners should understand that an effective mobile security solution combines security and systems management functionality from a single console.

Higher National Unit support notes (cont)

Unit title: Mobile Device Management (MDM) and Mobile Application Management (MAM): Introduction (SCQF level 8)

Mobile Device Management (MDM) is a centralised system aimed at controlling device configuration. Introducing learners to different types of MDM systems that are cloud based/hosted or in-house/on-premise will allow them to evaluate and configure key features of a Mobile Device Management solution such as cross-platform devise support, configuration management, device monitoring, license control, software distribution, inventory and asset control, remote control, connection management, scheduling and prioritisation, process automation, document and content distribution and bandwidth optimisation.

Mobile Application Management (MAM) focuses on provisioning, controlling and maintaining mobile applications on mobile devices and its main purpose is to provide public and internally developed applications to end users automatically. Discussions should focus on the key features of a Mobile Application Management solution such as distributing, securing, and tracking the organisation's mobile applications. Learners should be encouraged to use and configure the following functionalities of a MAM system:

- Install, update, and remove managed applications remotely
- Install required applications automatically during enrolment
- Allow users to install applications on-demand from the enterprise app catalogue
- Configure application access based on assignment rules
- Restrict application usage by creating blacklists, whitelists, and application compliance policies
- Restrict access to pre-installed applications on a device
- Disable iTunes, Google, or other public application stores
- Prevent data backup and automatically remove applications
- Track and view installed, approved, and blacklisted applications at the device and user level
- Receive alerts when an end user has installed an unapproved application
- Generate application inventory, version history, and compliance reports

Guidance on approaches to delivery of this unit

Delivery of the unit would be best served by completing each outcome in order.

A suggested distribution of time, across the outcomes, is:

Outcome 1, 2, 3 and 4 20 hours
Outcome 5 20 hours

During the delivery of this unit it is important that every opportunity is taken to introduce real-world examples, opportunities for whole-class and group discussion and practical demonstrations. Concepts and terminology should be presented in context throughout the unit. Video presentations should be used where appropriate for providing an alternative explanation of a difficult topic, or as a focus for class discussion or group work.

Higher National Unit support notes (cont)

Unit title: Mobile Device Management (MDM) and Mobile Application Management (MAM): Introduction (SCQF level 8)

It is recommended that centres could use during the delivery of the unit and assessments open source MDM and MAM solution such as Meraki Cisco, Miradore, OneMDM, etc. that could be installed and configured on different mobile devices using different operating systems. Introducing learners to more than one MDM/MAM system would allow them to evaluate different features and implementations of such systems. When any practical work is carried out it is advisable, time permitting, that a fault finding element be added into the teaching, thus enabling deeper learning.

Although not formally taught in this unit, learners should be aware of the Data Protection Act (1998) and Computer Misuse Act (1999) and also, the advantages of MDM/MAM systems to businesses and organisations.

Guidance on approaches to assessment of this unit

Evidence can be generated using different types of assessment. The following are suggestions only. There may be other methods that would be more suitable to learners.

Outcomes 1, 2, 3 and 4 could be assessed by means of a report that could be incorporate as part of a case study. The topics covered could be delivered in such a way that the practical uses and implications of the content of the outcome are made clear to learners. However, there is scope for the outcomes to be completed digitally. This could be achieved through a video recorded presentation or an auditory report.

The remaining outcome should be assessed via a project/case study. The practical elements from Outcome 5 may be done as individual tasks or carried out as part of a larger case study/project requirement the latter being advisable as it may lead to an enriched learner experience.

Integration of Outcomes 1, 2, 3, 4 and 5 will provide a more holistic approach more akin to the implementation of a MDM/MAM system. This unit could be wholly integrated and assessed using a case study or project based that would allow learners to investigate, implement and configure a small MDM/MAM system. The assessment for Outcomes 1, 2, 3 and 4 could be used as formative exercises.

Learners should develop research techniques in sourcing information.

This is an open-book assessment that should take place in a supervised or partly supervised environment. Assessors must assure themselves of the authenticity of each learner's submission. Reference will be permitted to textbooks, hand-outs or other material that learners have prepared for themselves.

Centres are reminded that prior verification of centre-devised assessments would help to ensure that the national standard is being met. Where learners experience a range of assessment methods, this helps them to develop different skills that should be transferable to work or further and higher education.

Higher National Unit support notes (cont)

Unit title: Mobile Device Management (MDM) and Mobile Application Management (MAM): Introduction (SCQF level 8)

Opportunities for e-assessment

E-assessment may be appropriate for some assessments in this unit. By e-assessment we mean assessment which is supported by Information and Communication Technology (ICT), such as e-testing or the use of e-portfolios or social software. Centres which wish to use e-assessment must ensure that the national standard is applied to all learner evidence and that conditions of assessment as specified in the evidence requirements are met, regardless of the mode of gathering evidence. The most up-to-date guidance on the use of e-assessment to support SQA's qualifications is available at **www.sqa.org.uk/e-assessment**.

Opportunities for developing Core and other essential skills

This unit would not normally develop Core Skills. This would be dependent on specific teaching and or assessment methods and as methods used on this unit are not prescriptive this unit could not guarantee inclusion of Core Skills.

History of changes to unit

Version	Description of change	Date

General information for learners

Unit title: Mobile Device Management (MDM) and Mobile Application Management (MAM): Introduction (SCQF level 8)

This section will help you decide whether this is the unit for you by explaining what the unit is about, what you should know or be able to do before you start, what you will need to do during the unit and opportunities for further learning and employment.

This unit is designed to provide you with knowledge of Mobile Device Management and Mobile Application Management technologies that enable secure smartphone and tablet use in business and organisations. This unit is split into two main sections. The first section is theoretical covering many aspects surrounding Mobile Device Management and Mobile Application Management technologies, such as factors involved in maintaining the reliability and security of data and devices in a MDM and MAM system, key features of a Mobile Device Management and Mobile Application Management solution, and security issues and solutions provided by Mobile Device Management (MDM) and Mobile Application Management (MAM) systems. The second section is practical and focuses on the implementation and configuration of a Mobile Device Management and Mobile Application Management system.

While studying this unit you will gain knowledge on the typical mobile devices that have second generation enterprise mobility capabilities and are used in business environment. You will learn about different types of mobile devices and mobile operating systems, types of networking such as WPAN, WLAN, WWAN, or satellite, and how data transferred from the mobile application to the enterprise server is done. Also, you will investigate and learn about Mobile Device Management/Mobile Application Management architecture.

You will also gain knowledge on various Mobile Device Management (MDM) systems. You will learn about cloud based/hosted or in-house/on-premise MDM systems and you will evaluate and configure key features of a Mobile Device Management solution.

Finally, you will be introduced to the challenges that organisations are forced to face when integrating mobile devices in their existing information and communication infrastructures. You will learn about possible vulnerabilities and security leaks. You will also learn about effective mobile security solution such as password protection, on-device data encryption, data-fading, over the air data encryption, patch management.

To complete this unit successfully, you will have to achieve a satisfactory level of performance in both the theoretical and practical outcomes of the unit. You may be assessed for your knowledge through a report and practical skills via a project/case study. The assessments will be open-book and you will be allowed access to paper-based and online resources during the assessments.