Higher Nationals

Computing (Cyber Security)

YES PROFESSIONAL ADVANCEMENT CENTER

Specification

For use with the Higher National Certificate and Higher National Diploma in Computing

First teaching from September 2022
First Certification from September 2023

Higher National Certificate Lvl 4

Higher National Diploma Lvl 5

Pearson BTEC

Units for HNC Computing (Cyber Security) – HCMB9

SN	U N	UNIT	Code	Type	Level	Credit
1	1	Programming	H/618/7388	Core	4	15
2	2	Networking	M/618/7393	Core	4	15
3	3	Professional Practice	L/618/739	Core	4	15
4	4	Database Design & Development	A/618/7400	Core	4	15
5	5	Security	D/618/7406	Core	4	15
6	6	Planning a Computing Project	H/618/7407	Core	4	15
7	10	Cyber Security	M/618/5661	Core	4	15
8	14	Maths for Computing	R/618/7421	Optional	4	15

Units for HND Computing (Cyber Security) – HCMC6

SN	U N	UNIT	Code	Type	Level	Credit
9	16	Computing Research Project	K/618/7425	Core	5	30
10	17	Business Process Support	A/618/7428	Core	5	15
11	30	Applied Cryptography in the Cloud	F/618/4899	Core	5	15
12	31	Forensics	T/618/7444	Core	5	15
13	32	Information Security Management	J/618/7447	Core	5	15
14	18	Discrete Maths	F/618/7429	Optional	5	15
15	26	Big Data Analytics and Visualisation	F/618/5664	Optional	5	15

Unit 1: Programming

Unit code	**H/618/7388**
Unit type	**Core**
Unit level	**4**
Credit value	**15**

Introduction

Programming involves describing processes and procedures that are derived from algorithms. The ability to program is what sets apart a developer and an end user. Typically, the role of the developer is to instruct a device (such as a computer) to carry out instructions; the instructions are known as source code and are written in a language that is converted into something the device can understand. The device executes the instructions it is given.

Algorithms help to describe the solution to a problem or task by identifying the data and the process needed to represent the problem or task *and* the set of steps needed to produce the desired result. Programming languages typically provide the representation of both the data and the process; they provide control constructs and data types (which can be numbers, words and objects, and be constant or variable). The control constructs are used to represent the steps of an algorithm in a convenient yet unambiguous fashion. Algorithms require constructs that can perform sequential processing, selection for decision making and iteration for repetitive control. Any programming language that provides these basic features can be used for algorithm representation.

This unit introduces students to the core concepts of programming along with an introduction to algorithms and the characteristics of programming paradigms. Among the topics included in this unit are: introduction to algorithms, procedural, object-orientated and event-driven programming, security considerations, the integrated development environment and the debugging process.

On successful completion of this unit, students will be able to design and implement algorithms in a chosen language in a suitable Integrated Development Environment (IDE). This IDE will be used to develop and help track any issues with the code. As a result, students will develop skills such as communication literacy, critical thinking, analysis, reasoning and interpretation, which are crucial for gaining employment and developing academic competence.

Learning Outcomes

By the end of this unit students will be able to:

LO1 Define basic algorithms to carry out an operation and outline the process of programming an application

LO2 Explain the characteristics of procedural, object-orientated and event-driven programming

LO3 Implement basic algorithms in code using an IDE

LO4 Determine the debugging process and explain the importance of a coding standard.

Essential Content

LO1 Define basic algorithms to carry out an operation and outline the process of programming an application

Algorithm definition:

Writing algorithms to carry out an operation, e.g. Bubble sort.

The relationship between algorithms and code.

The generation process of code; the roles of the pre-processor, compiler and linker, interpreter.

LO2 Explain the characteristics of procedural, object-orientated and event-driven programming

Characteristics of code:

Definitions of: data types (the role of constants/variables), data structures, e.g. arrays, stacks, queues, methods (including input/output), control structures, iteration, scope, parameter passing, classes, inheritance and events.

Key components of an IDE, with a brief explanation of each component.

Use of addition of advanced text editors to view code, such as Notepad++, Atom, Sublime Text etc.

LO3 Implement basic algorithms in code using an IDE

Implementation:

Develop simple applications that implement basic algorithms, including the features of a suitable language and IDE.

Create logical and maintainable codes.

Consideration of security concerns and how they could be solved.

Build, manage and deploy code to the relevant environment to solve the identified problems.

LO4 **Determine the debugging process and explain the importance of a coding standard**

Review and reflection:

Documentation of the debugging process in the IDE, with reference to watch lists, breakpoints and tracing.

Use of debugging the process to help developers fix vulnerabilities, defects and bugs in code.

Apply structured techniques to problem solving, debugging code and consider structure of programmes to identify and resolve issues.

Understand coding standards and their benefits when writing code.

Learning Outcomes and Assessment Criteria

Pass	Merit	Distinction
LO1 Define basic algorithms to carry out an operation and outline the process of programming an application		
P1 Define an algorithm and outline the process in building an application. **P2** Determine the steps taken from writing code to execution.	**M1** Analyse the process of writing code, including the potential challenges faced.	**D1** Evaluate the implementation of an algorithm in a suitable language and the relationship between the written algorithm and the code variant.
LO2 Explain the characteristics of procedural, object-orientated and event-driven programming		
P3 Discuss what procedural, object-orientated and event-driven paradigms are; their characteristics and the relationship between them.	**M2** Compare the procedural, object-orientated and event-driven paradigms used in given source code of an application.	**D2** Critically evaluate the source code of an application that implements the procedural, object-orientated and event-driven paradigms, in terms of the code structure and characteristics.
LO3 Implement basic algorithms in code using an IDE		
P4 Write a program that implements an algorithm using an IDE.	**M3** Enhance the algorithm written, using the features of the IDE to manage the development process.	**D3** Evaluate the use of an IDE for development of applications contrasted with not using an IDE.
LO4 Determine the debugging process and explain the importance of a coding standard		
P5 Explain the debugging process and the debugging facilities available in the IDE. **P6** Explain the coding standard you have used in your code.	**M4** Examine how the debugging process can be used to help develop more secure, robust applications.	**D4** Evaluate the role and purpose of a coding standard and why it is necessary in a team as well as for the individual.

Recommended Resources

This unit does not specify which programme language should be used to deliver the content – this decision can be made by the tutor.

Examples of languages that are used in industry are C#, Python, Ruby and Java, but any language that will allow students to achieve the Learning Outcomes is acceptable.

Textbooks

Aho, A. V. et al. (1987) *Data Structures and Algorithms*. 1st edn. Addison-Wesley.

Hunt, A. et al. (2000) *The Pragmatic Programmer: From Journeyman to Master.* 1st edn. Addison-Wesley.

McConnell, S. (2004) *Code Complete: A Practical Handbook of Software Construction.* 2nd edn. Microsoft Press.

Links

This unit links to the following related units:

Unit 19: Data Structures & Algorithms

Unit 20: Applied Programming and Design Principles

Unit 54: Prototyping.

Unit 2: Networking

Unit code	**M/618/7393**
Unit type	**Core**
Unit level	**4**
Credit value	**15**

Introduction

Computer networks are the driving force behind the evolution of computer systems and allow users to access data, hardware, and services regardless of their location. Being knowledgeable about the underlying principles of networking is of vital importance to all IT professionals. Networking is an environment that is increasingly complex and under continuous development.

Complex computer networking has connected the world by groups of small networks through internet links to support global communications. It supports access to digital information any time, anywhere, using many applications like email, audio and video transmission, including the World Wide Web, and this has opened the floodgates to availability of information.

The aim of this unit is to give students a wider background knowledge of computer networking essentials, how they operate, protocols, standards, security considerations and the prototypes associated with a range of networking technologies. Students will explore a range of hardware, with related software, and will configure and install these to gain knowledge of networking systems. A range of networking technologies will be explored to deliver a fundamental knowledge of Local Area Networking (LAN), Wide Area Networking (WAN) and their evolution to form large-scale networks. Students will also explore the protocol methodologies related to IP data networks.

On successful completion of this unit, students will have gained the knowledge and skills needed to successfully install, operate and troubleshoot a small network; and the operation of IP data networks, router, switching technologies, IP routing technologies, IP services and basic troubleshooting. Supporting a range of units in the Higher National suite, this unit underpins the principles of networks for all and enables students to work towards their studies in vendor units, if applicable. Students will develop skills such as communication literacy, critical thinking, analysis, reasoning and interpretation, which are crucial for gaining employment and developing academic competence.

Learning Outcomes

By the end of this unit students will be able to:

LO1 Examine networking principles and their protocols

LO2 Explain networking devices and operations

LO3 Design efficient networked systems

LO4 Implement and diagnose networked systems.

Essential Content

LO1 Examine networking principles and their protocols

Introduction to networks:

Impact of networks on daily lives, the basic requirements of a reliable network, employment opportunities in the networking field, network common network attacks, network trends, e.g. bring your own device (BYOD).

Role of networks:

Purpose, benefits, resource implications, communications, e.g. transmission mediums, working practice, commercial opportunity, information sharing, collaboration.

System types:

Peer-based, client-server, cloud, cluster, centralised, virtualised.

Networking standards:

Conceptual models, e.g. OSI model, TCP/IP model; standards, e.g. IEEE 802.x.

Topology:

Network representation logical, e.g. ethernet, Token Ring; physical, e.g. star, ring, bus, mesh, tree.

Protocols:

Purpose of protocols; adherence, routed protocols, e.g. IPv4 (addressing, subnetting, VLSM), IPv6 (addressing); global unicast, multicast, link local, unique local, EUI 64, auto configuration, ICMP, FTP, HTTP, SMTP, POP3, SSL; management of protocols for addressing.

Wireless networks:

Explore the use and evolution and industry developments in mobile/cellular networks, including key technologies; standards for communications (3G, 4G, 5G); process of accessing and connecting to NB-IoT, GPRS and Wi-Fi networks.

Distinguish between NB-IoT and Wi-Fi AT command sets.

LO2 **Explain networking devices and operations**

Networking devices:

Explain the operation of server, hub, routers, switches, multilayer switch (including their operating systems, e.g. CISCO IOS, etc.), firewall, Host-based Intrusion System (HIDS), repeaters, bridges, wireless devices, access point (wireless/wired), content filter, load balancer, modem, packet shaper, VPN concentrator.

Explore the basic concepts, features and key technologies of IoT gateways, including IoT gateway solutions, industrial IoT gateway positioning, edge computing, network topologies, RF mesh, Smart Home networks, acceleration, Wi-Fi coverage and intelligent services and serial data transmission (binary data).

Networking software:

Client software, server software, client operating system, server operating system, firewall.

Server type:

Web, file, database, combination, virtualisation, terminal services server.

Server selection:

Cost, purpose, operating system requirement.

Workstation:

Hardware, e.g. network card, cabling.

System bus and local-system architecture, e.g. memory, processor, I/O devices.

Permissions.

LO3 **Design efficient networked systems**

Bandwidth:

Expected average load, anticipated peak load, local internet availability, cost constraints, throughput.

Users:

Quality expectations, concept of system growth.

Consider what the network will be used for (purpose) according to the scenario.

Networking services and applications:

DHCP, including static vs dynamic IP addressing, reservations, scopes, leases, options (DNS servers, Suffixes), IP helper, DHCP relay, DNS records, Dynamic DNS, static and dynamic routing between multiple subnets.

Calculate IP subnet address ranges in dotted decimal and binary.

Calculate subnet masks.

Communications:

Ensuring communications are suited to devices, suited to users, supportive of lifestyle desires, supportive of commercial requirements, security requirements, quality of service needs.

Scalability:

Ability to support device growth, able to support addition of communication devices, able to cope with bandwidth use and trend changes, protocol utilisation, addressing, multiple subnets, dynamic, static routing protocols.

Selection of components:

Supporting infrastructure needs; supporting connectivity requirements.

Security:

The concept of 'secure by design' and its application to infrastructure.

Security considerations when designing a network for an identified scenario, e.g. shared data, network access, remote workers, public facing systems, internal policy.

LO4 **Implement and diagnose networked systems**

Devices:

Installation of communication devices, allocation of addresses, local client configuration, server configuration, server installation, security considerations.

Verification of configuration and connectivity:

Installation of internet work communication medium, ping, extended ping, traceroute, telnet, SSH.

Evidence the system meets design requirements, including security controls as required by the scenario, have been implemented.

System monitoring:

Utilisation, bandwidth needs, monitoring user productivity and security of the system. Factors affecting network performance.

Identify typical failure modes in protocols and approaches to error control.

Review network monitoring data to optimise performance and undertake root cause analysis of events and make recommendations to reduce false positives and false negatives.

Network automation:

Process of setting up software to automatically manage, configure, test, deploy, and operate network devices (physical or virtual).

Maintenance schedule:

Backups, upgrades, security, auditing.

Diagnose and resolve layer 1 problems:

Explore the E2E integrated development and testing process.

Framing, CRC, runts, giants, dropped packets, late collisions, input/output errors.

Policy review:

Bandwidth, resource availability.

Service level agreements (SLAs):

Conditions of service availability, time window for each level of service (prime time and non-prime time), responsibilities of each party, escalation procedures, and cost/service trade-offs.

Learning Outcomes and Assessment Criteria

Pass	Merit	Distinction
LO1 Examine networking principles and their protocols		
P1 Discuss the benefits and constraints of different network types and standards. **P2** Explain the impact network topologies have on communication and bandwidth requirements.	**M1** Assess common networking principles and how protocols enable the effectiveness of networked systems.	**D1** Evaluate the topology and protocol suite selected for a given scenario and how it demonstrates the efficient utilisation of a networking system.
LO2 Explain networking devices and operations		
P3 Discuss the operating principles of networking devices and server types. **P4** Discuss the interdependence of workstation hardware and relevant networking software.	**M2** Explore a range of server types and justify the selection of a server for a given scenario, regarding cost and performance optimisation.	
LO3 Design efficient networked systems		
P5 Design a networked system to meet a given specification. **P6** Design a maintenance schedule to support the networked system.	**M3** Analyse user feedback on your designs with the aim of optimising your design and improving efficiency.	**D2** Critically reflect on the implemented network, including the design and decisions made to enhance the system.
LO4 Implement and diagnose networked systems		
P7 Implement a networked system based on a prepared design. **P8** Document and analyse test results against expected results.	**M4** Recommend potential enhancements for the networked systems.	

Recommended Resources

Textbooks

Burgess, M. (2003) *Principles of Network and System Administration*. 2nd edn. John Wiley and Sons Ltd.

Donahue, G. A. (2011) *Network Warrior* 2nd edn. O'Reilly Media.

Goransson, P. Black, C. et al (2016) *Software Defined Networks: A Comprehensive Approach* 2nd edn. Morgan Kaufmann.

Hallberg, B. (2005) *Networking: A Beginner's Guide*. 4th edn. Osborne/McGraw-Hill US.

Limoncelli, T. and Hogan, C. (2001) *The Practice of System and Network Administration*. Addison-Wesley.

Lowe, D. (2005) *Networking All-in-One Desk Reference for Dummies.* 2nd edn. Hungry Minds Inc.

Olifer, N. and Olifer, V. (2005) *Computer Networks: Principles, Technologies and Protocols for Network Design.* John Wiley and Sons Ltd.

Stallings, W. (2003) *Data and Computer Communications*. 7th edn. (Prentice Hall).

Tanenbaum, A. (2002) *Computer Networks*. Prentice Hall PTR.

Links

This unit links to the following related units:

Unit 9: Computer Systems Architecture

Unit 27: Transport Network Design

Unit 29: Network Security

Unit 39: Network Management

Unit 40: Client/Server Computing Systems.

Unit 3: Professional Practice

Unit code	**L/618/7398**
Unit type	**Core**
Unit level	**4**
Credit value	**15**

Introduction

In the workplace, it is essential to be effective as a communicator, critical thinker, analyser, team worker and team leader. These skills are needed on a daily basis in order to carry out designated tasks as part of a job role. The development of academic competence and the continuation of lifelong learning and continuing professional development (CPD) are required to ensure that individuals have a valued set of interpersonal skills that can be applied to any situation or environment.

This unit provides a foundation for good practice in a variety of contexts. The ability to communicate effectively using different tools and mediums will ensure that practical, research, design, reporting and presentation tasks are undertaken professionally and in accordance with various communication conventions. In everyday life, the ability to apply critical reasoning and solve problems are skills that enable tasks to be completed successfully and facilitate effective decision making. Working with others in a group environment such as an academic setting or in the workplace is an integral part of everyday life. Therefore, understanding the dynamics of teams in terms of culture, roles and responsibilities will ensure that there is a better understanding and awareness of the importance and value of teamwork. Continuing professional development, self-improvement, reflective practice and working towards various goals are encouraged in the workplace through an appraisal framework. Professional development includes at higher levels of learning and the ability to demonstrate effective research skills and academic reporting skills.

This unit covers the development of communication skills and communication literacy and the use of qualitative and quantitative data to demonstrate analysis, reasoning and critical thinking. Students will carry out tasks that require working with others in a team-based scenario and planning and problem solving.

On successful completion of the unit, students will be able to demonstrate leadership skills through the dynamics of team working. Through reflective practice, they will be able to evaluate the contributions they make as an individual and those of others.

Learning Outcomes

By the end of this unit students will be able to:

LO1 Demonstrate a range of interpersonal and transferable communication skills to a target audience

LO2 Apply critical reasoning and thinking to a range of problem-solving scenarios

LO3 Discuss the importance and dynamics of working within a team and the impact of team working in different environments

LO4 Examine the need for continuing professional development (CPD) and its role within the workplace and for higher-level learning.

Essential Content

LO1 Demonstrate a range of interpersonal and transferable communication skills to a target audience

Effective communication:

Verbal and non-verbal, e.g. awareness and use of body language, openness and responsiveness, formal and informal dialogue and feedback to a range of different stakeholders, academic report writing, use of IT to enhance communication, use of source information to undertake research.

Understanding of the reasons for communicating with internal and external stakeholders, e.g. responding to queries, technical support, providing instructions, raising awareness of issues.

Considerations when communicating with internal and external stakeholders, e.g. maintaining privacy and security, tone of voice, use of technical vocabulary or jargon, company image.

Consideration of issues relating to inclusion and diversity when communicating and interacting with others.

Interpersonal skills:

Soft skills, e.g. personal effectiveness, working with others, use of initiative, negotiating skills, assertiveness skills and social skills.

Time-management skills:

Prioritising workloads, setting objectives, using time effectively, making and keeping appointments, planning and scheduling tasks and activities.

LO2 Apply critical reasoning and thinking to a range of problem-solving scenarios

Specification of the problem:

Definition of the problem; analysis and clarification.

Identification of possible outcomes:

Identification and assessment of various alternative outcomes.

Tools and methods:

Use of problem-solving methods and tools.

Demonstrate resourcefulness and creativity when solving problems.

Plan and implement:

Sources of information, solution methodologies, selection and implementation of the best corrective action, e.g. timescale, stages, resources, critical path analysis.

Evaluation:

Evaluation of problem solving, measurement of solution against specification and desired outcomes, sustainability.

LO3 **Discuss the importance and dynamics of working within a team and the impact of team working in different environments**

Working with others:

Nature and dynamics of team and group work, informal and formal settings.

Purpose of teams and groups, e.g. long-term corporate objectives and strategy, problem-solving and short-term development projects, flexibility and adaptability, team player.

Individual responsibility when working as part of a team.

Working effectively on individual and collaborative tasks regardless of levels of supervision.

Allocation and management of tasks between members of the team, identifying team members' strengths, communicating requirements and expectations effectively.

Teams and team building:

Selecting team members e.g. specialist roles, skill and style/approach mixes.

Identification of team and work group roles.

Stages in team development, including team building, identity, loyalty, commitment to shared beliefs, professionalism.

Team health evaluation, including promoting and maintaining a safe and secure working environment, action planning, monitoring and feedback, coaching skills, ethics.

Effective leadership skills, e.g. setting direction, setting standards, motivating, innovative, responsive, effective communicator, reliability, consistency.

LO4 **Examine the need for continuing professional development (CPD) and its role within the workplace and for higher-level learning**

Responsibilities:

Own responsibilities, e.g. personal responsibility, direct and indirect relationships and adaptability, decision-making processes and skills, ability to learn and develop within the work role.

Other responsibilities, including employment legislation, ethics, employment rights and responsibilities.

Maintaining a productive, professional and secure working environment.

Performance objectives:

Setting and monitoring performance objectives, measurement tools for success and achievement.

CPD, including lifelong learning, training and development, personal development, professional development.

Evidence criteria:

Production data, personnel data, judgemental data.

Rating methods, e.g. ranking, paired comparison, checklist, management by objectives.

Skills audit, including personal profile using appropriate self-assessment tools, evaluating self-management.

Personal and interpersonal skills.

Motivation and performance:

Application and appraisal of motivational theories and techniques, rewards and incentives; manager's role; self-motivational factors.

Development plan:

Plan to include current performance, future needs, opportunities and threats to career progression, aims and objectives, achievement dates, review dates, learning programme or activities, action plans, personal development plans, ongoing commitment to CPD.

Learning Outcomes and Assessment Criteria

Pass	Merit	Distinction
LO1 Demonstrate a range of interpersonal and transferable communication skills to a target audience		
P1 Demonstrate effective design and delivery of a training event for a given target audience, using different communication styles and formats. **P2** Demonstrate effective time-management skills in planning an event.	**M1** Design a professional schedule to support the planning of an event, to include contingencies and justifications of time allocated.	**D1** Evaluate the effectiveness and application of interpersonal skills used in the design and delivery of a training event.
LO2 Apply critical reasoning and thinking to a range of problem-solving scenarios		
P3 Demonstrate the use of different problem-solving techniques in the design and delivery of an event. **P4** Demonstrate that critical reasoning has been applied to the design and delivery of the event.	**M2** Research the use of different problem-solving techniques used in the design and delivery of an event. **M3** Justify the use and application of a range of methodologies in the design and delivery of an event.	**D2** Evaluate the overall success of the event delivered, in terms of how well critical reasoning and thinking were applied to achieve the end goal.

Pass	Merit	Distinction
LO3 Discuss the importance and dynamics of working within a team and the impact of team working in different environments		
P5 Discuss the importance of team dynamics in the success and/or failure of group work. **P6** Work in a team to achieve a defined goal.	**M4** Analyse team dynamics, in terms of the roles that group members play in a team and the effectiveness in terms of achieving shared goals.	**D3** Critically evaluate your own role and contribution to a group scenario.
LO4 Examine the need for Continuing Professional Development (CPD) and its role within the workplace and for higher-level learning		
P7 Discuss the importance of CPD and its contribution to own learning and motivation. **P8** Review different motivational theories and the impact they can have on performance in the workplace. **P9** Produce a development plan that outlines responsibilities, performance objectives and required skills for future goals.	**M5** Justify the role of CPD and development planning in building motivation.	**D4** Evaluate a range of evidence criteria that is used as a measure for effective CPD.

Recommended Resources

Textbooks

Cottrell, S. (2001*) Critical Thinking Skills: Developing Effective Analysis and Argument.* 2nd edn. Palgrave Macmillan.

Forde, C. et al (2006) *Professional Development, Reflection and Enquiry.* Sage Publications.

Megginson, D. and Whitaker, V. (2007) *Continuing Professional Development*. 2nd edn. Chartered Institute of Personnel and Development.

Winstanley, D. (2005) *Personal Effectiveness: A guide to action.* Chartered Institute of Personnel and Development.

Journals

Journal of Group Dynamics – Japan Institute for Group Dynamics

Professional Development in Education – Taylor and Francis Online

Web

ipda.org.uk	International Professional Development Association (General Reference)
www.thinkwatson.com	Critical Thinking Resources *Critical Thinking Correlation Studies* (Research)

Links

This unit links to the following related units:

Unit 6: Planning a Computing Project (Pearson-set)

Unit 16: Computing Research Project (Pearson-set).

Unit 4: Database Design & Development

Unit code	**A/618/7400**
Unit type	**Core**
Unit level	**4**
Credit value	**15**

Introduction

Organisations depend on their databases for providing information that is essential for their day-to-day operations and to help them take advantage of today's rapidly growing and maturing e-commerce opportunities. An understanding of database tools and technologies is an essential skill for designing and developing systems to support them.

As applications get increasingly more sophisticated, database systems continue to demand more complex data structures and interfaces. Most organisations collect and store large volumes of data, either on their own systems or in the cloud, and this data is used not just for the operational running of their business but is also mined for other more intelligent and complex applications. Databases stand as the back-end of most systems used by organisations for their operations.

Database design and development is a fundamental and highly beneficial skill for computing students to master, regardless of their specialism.

The aim of this unit is to give students opportunities to develop an understanding of the concepts and issues relating to database design and development. It will also provide the practical skills needed to be able to translate that understanding into the design and creation of complex databases.

Topics covered in this unit are: examination of different design tools and techniques; examination of different development software options; consideration of the development features of a fully-functional robust solution covering data integrity, data validation, data consistency, data security and advanced database querying facilities across multiple tables; appropriate user interfaces for databases and for other externally linked systems; creating complex reports/dashboards, testing the system against the user and system requirements; and elements of complete system documentation.

On successful completion of the unit, students will be able to use appropriate tools to design and develop a relational database system for a substantial problem. They will be able to test the system to ensure that it meets user and system requirements, and fully document the system by providing technical and user documentation. For practical purposes, this unit covers relational databases and related tools and techniques. A brief overview of object-oriented databases will also be covered. As a result, students will develop skills such as communication literacy, critical thinking, analysis, reasoning and interpretation, which are crucial for gaining employment and developing academic competence.

Learning Outcomes

By the end of this unit students will be able to:

LO1 Use an appropriate design tool to design a relational database system for a substantial problem

LO2 Develop a fully-functional relational database system, based on an existing system design

LO3 Test the system against user and system requirements

LO4 Produce technical and user documentation.

Essential Content

LO1 Use an appropriate design tool to design a relational database system for a substantial problem

Database design:

Principles and uses of relational and non-relational databases.

The role of database systems, e.g. as back-end systems, in e-commerce, for data mining applications, blockchain.

Determining user and system requirements.

Design tools and techniques for a relational database system.

Logical design for relational databases, including structured data in tables, data elements, data types, indexes, primary and foreign keys, entity relationship modelling, referential integrity, data normalisation to third normal form.

Designs for data integrity, data validations, data security and data controls. User interface design.

Output designs for user requirements.

Overview of object-oriented databases and their design tools.

LO2 Develop a fully-functional relational database system, based on an existing system design

Implementation:

Consideration of database and platform options for system development.

Examination of different software development options for developing the relational database system.

Implementation of the physical data model based on the logical model and linking code to data sets.

Data stores, internal storage and external storage, e.g. the cloud.

Implementation of security elements in databases.

Relational databases with controls like data validation using; input masks, dropdown lists, option buttons.

Consideration of user interface requirements looking at functionality, reliability, consistency, performance and accessibility for a range of different users.

Develop effective user interfaces linked with other systems, e.g. internet-based applications.

Data manipulation using appropriate query tools, including complex queries to query across multiple tables and using functions and formulae.

Database maintenance and data manipulation: inserts, updates, amendments, deletions, data backup and recovery.

System reports using report-writing tools and report generators, dashboards.

Implementation of security elements in a database, including consideration of permissions, access rights, network vulnerabilities, physical location of data, multi-tenancy and data separation, encryption.

Consideration of GDPR issues, including data crossing borders and other nations' data protection regulations.

LO3 **Test the system against user and system requirements**

Testing methodologies:

Identify elements of the system that need to be tested. Consider data that should be used to fully test the system.

Match tests against user and system requirements.

Test procedures to be used: test plans, test models, e.g. white box, black box; testing documentation.

Functional and system testing and testing the robustness of the system, including help menus, pop-ups, hot-spots, data validation checks.

LO4 **Produce technical and user documentation**

Structure and functionality documentation:

Technical and user documentation and their contents.

Technical documentation to include diagrams showing movement of data through the system and flowcharts describing how the system works.

User documentation, including how to use the system, outputs produced by the system, menu operations and other functions.

Learning Outcomes and Assessment Criteria

<table>
<tr><th>Pass</th><th>Merit</th><th>Distinction</th></tr>
<tr><td colspan="2">LO1 Use an appropriate design tool to design a relational database system for a substantial problem</td><td rowspan="2">D1 Evaluate the effectiveness of the design in relation to user and system requirements.</td></tr>
<tr><td>P1 Design a relational database system using appropriate design tools and techniques, containing at least four interrelated tables, with clear statements of user and system requirements.</td><td>M1 Produce a comprehensive design for a fully-functional system, which includes interface and output designs, data validations and data normalisation.</td></tr>
<tr><td colspan="2">LO2 Develop a fully-functional relational database system, based on an existing system design</td><td rowspan="4">D2 Evaluate the effectiveness of the database solution in relation to user and system requirements and suggest improvements.</td></tr>
<tr><td>P2 Develop the database system with evidence of user interface, output and data validations, and querying across multiple tables.
P3 Implement a query language into the relational database system.</td><td>M2 Implement a fully-functional database system, which includes system security and database maintenance.
M3 Assess whether meaningful data has been extracted through the use of query tools to produce appropriate management information.</td></tr>
<tr><td colspan="2">LO3 Test the system against user and system requirements</td></tr>
<tr><td>P4 Test the system against user and system requirements.</td><td>M4 Assess the effectiveness of the testing, including an explanation of the choice of test data used.</td></tr>
</table>

Pass	Merit	Distinction
LO4 Produce technical and user documentation		
P5 Produce technical and user documentation.	**M5** Produce technical and user documentation for a fully-functional system, including data flow diagrams and flowcharts, describing how the system works.	**D3** Evaluate the database in terms of improvements needed to ensure the continued effectiveness of the system.

Recommended Resources

Textbooks

Churcher, C. (2012) *Beginning Database Design: From Novice to Professional.* 2nd edn. Apress.

Connolly, T. and Begg, C. (2014) *Database Systems: A Practical Approach to Design, Implementation and Management*. 6th edn. Global Edition. Pearson.

Flejoles, R. P. (2018) *Database Theory and Application*. Arcler Press.

Karwin, B. (2017) *SQL Antipatterns: Avoiding the Pitfalls of Database Programming* Pragmatic Programmers, LLC, The.

Kroemke, D. and Auer, D. (2012) *Database Concepts: International Edition.* 6th edn. Pearson.

Journals

The Computer Journal – Oxford Academic

International Journal of Database Management (IJDMS)

Journal of Emerging Trends in Computing and Information Sciences

Journal of Systems Analysis and Software Engineering

Systems Journal of Database Management

Web

mva.microsoft.com	Microsoft Virtual Academy Database Development (Training)
mva.microsoft.com/ebooks	Microsoft Virtual Academy Microsoft Press (E-books)
www.lynda.com	Database Training (Tutorials)

Links

This unit links to the following related units:

Unit 11: Strategic Information Systems

Unit 41: Database Management Systems.

Unit 5: Security

Unit code	**D/618/7406**
Unit type	**Core**
Unit level	**4**
Credit value	**15**

Introduction

Security is one of the most important challenges modern organisations face. It is about protecting organisational assets, including personnel, data, equipment and networks, from attack through the use of prevention techniques in the form of vulnerability testing/security policies and detection techniques, exposing breaches in security and implementing effective responses.

The aim of this unit is to give students knowledge of security, the associated risks and how it has an impact on business continuity. Students will examine security measures involving access authorisation and regulation of use. They will implement contingency plans and devise security policies and procedures. The unit also introduces students to detection of threats and vulnerabilities in physical and IT security, and how to manage risks relating to organisational security.

This unit includes network security design and operational topics, including address translation, DMZ, VPN, firewalls, AV and intrusion detection systems. Remote access will be covered, as will the need for frequent vulnerability testing as part of organisational and security audit compliance. As a result, students will develop skills such as communication literacy, critical thinking, analysis, reasoning and interpretation, which are crucial for gaining employment and developing academic competence.

Learning Outcomes

By the end of this unit students will be able to:

LO1 Assess risks to IT security

LO2 Describe IT security solutions

LO3 Review mechanisms to control organisational IT security

LO4 Manage organisational security.

Essential Content

LO1 **Assess risks to IT security**

IT security risks:

Risks of unauthorised use of a system, including unauthorised removal or copying of data or code from a system, damage to or destruction of physical system assets and environment, damage to or destruction of data or code inside or outside the system, naturally occurring risks, internal and external sources of risk.

Legal restrictions on the access to data, including UK and international data laws (walled garden laws), e.g. General Data Protection Regulation (UK) (GDPR).

Organisational security, including business continuance, backup/restoration of data, audits, areas of systems to be secured, e.g. data, network, systems (hardware and software), WANs, intranets, wireless access systems, security culture and the approaches to security in the work place, operational impact of security breaches.

The concepts, main functions and features of a range of Operating Systems (OS) and their security functions and associated security features.

LO2 **Describe IT security solutions**

IT security solution evaluation:

Network security infrastructure, including evaluation of network address translation (NAT), demilitarized zone (DMZ), static and dynamic IP addresses.

Network performance: redundant array of inexpensive disks (RAID), Main/Standby, Dual LAN, web server balancing.

Data security, including asset management, image differential/incremental backups, storage area network (SAN) servers, encryption.

Data centre, including replica data centres, virtualisation, secure transport protocol, secure MPLS routing, segment routing and remote access methods/procedures for third-party access, physical mechanisms, e.g. air flow and cooling to prevent overheating.

Security vulnerability, including logs, traces, honeypots, data mining algorithms, vulnerability testing, zero-day exploits.

Educating staff and customers on IT security issues and prevention methods.

Understand how cyber security technology components are typically deployed in digital systems to provide security and functionality, including hardware and software to implement security controls.

LO3 **Review mechanisms to control organisational IT security**

Mechanisms to control organisational IT security:

Risk assessment and integrated enterprise risk management: network change management, audit control, business continuance/disaster recovery plans, potential loss of data/business, intellectual property, hardware and software.

Probability of occurrence, e.g. disaster, theft.

Staff responsibilities.

Legal mechanisms, both UK and international, including Data Protection Act 2018, Computer Misuse Act 1990 and amendments, ISO 31000 Risk Management standards.

Company regulations: site or system access criteria for personnel; physical security types, e.g. biometrics, swipe cards, theft prevention.

Awareness of common security architectures and methodologies that incorporate hardware and software components, and sources of architecture patterns and guidance.

Assess the security culture within an organisation (the approach to security, including how user actions impact on security).

Ensure system defences are informed by the most up-to-date legislation and guidance on best practice from professional bodies.

LO4 **Manage organisational security**

Manage organisational security:

Organisational security policies, e.g. system access, access to internet email, access to internet browser, development/use of software, physical access and protection, third-party access, business continuity, responsibility matrix.

Reviewing and monitoring of security risk assessments and ensuring stakeholder compliance with security procedures and standards.

Collect information from various sources (e.g. log files, system monitoring tools, Secure Information and Event Management (SIEM) tools, access control systems, physical security systems) and compare to known threat and vulnerability data to determine a digital system security breach.

Using enterprise risk management (as part of system management and lifecycle) for identifying, evaluating, implementing and follow up of security risks according to ISO 31000 standards.

Understand appropriate security tools and methods, e.g. user log-on profiles to limit user access to resources, online software to train and update staff.

Auditing tools to monitor resource access, security audits and penetration testing.

Investigate organisation policy on ethical hacking and bug bounties.

Gathering and recording information on security and initiating suitable actions for remediation.

Learning Outcomes and Assessment Criteria

<table>
<tr><th>Pass</th><th>Merit</th><th>Distinction</th></tr>
<tr><td colspan="2">LO1 Assess risks to IT security</td><td rowspan="4">D1 Evaluate a range of physical and virtual security measures that can be employed to ensure the integrity of organisational IT security.</td></tr>
<tr><td>P1 Discuss types of security risks to organisations.
P2 Assess organisational security procedures.</td><td>M1 Analyse the benefits of implementing network monitoring systems with supporting reasons.</td></tr>
<tr><td colspan="2">LO2 Describe IT security solutions</td></tr>
<tr><td>P3 Discuss the potential impact to IT security of incorrect configuration of firewall policies and third-party VPNs.
P4 Discuss, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve network security.</td><td>M2 Propose a method to assess and treat IT security risks.</td></tr>
<tr><td colspan="2">LO3 Review mechanisms to control organisational IT security</td><td rowspan="2">D2 Recommend how IT security can be aligned with an organisational policy, detailing the security impact of any misalignment.</td></tr>
<tr><td>P5 Review risk assessment procedures in an organisation.
P6 Explain data protection processes and regulations as applicable to an organisation.</td><td>M3 Summarise an appropriate risk-management approach or ISO standard and its application in IT security.
M4 Analyse possible impacts to organisational security resulting from an IT security audit.</td></tr>
</table>

Pass	Merit	Distinction
LO4 Manage organisational security		
P7 Design a suitable security policy for an organisation, including the main components of an organisational disaster recovery plan. **P8** Discuss the roles of stakeholders in the organisation in implementing security audits.	**M5** Justify the security plan developed giving reasons for the elements selected**.**	**D3** Evaluate the suitability of the tools used in the organisational policy to meet business needs.

Recommended Resources

Textbooks

Alexander, D. et al. (2020) *Information Security Management Principles.* BSC.

Collins, R. (2017) *Network Security Monitoring: Basics for Beginners. A Practical Guide* CreateSpace Independent Publishing Platform.

Sanders, C. Smith, J. (2013) *Applied Network Security Monitoring: Collection, Detection, and Analysis.* Syngress.

Steinberg, R. (2011) *Governance, Risk Management, and Compliance: It Can't Happen to Us – Avoiding Corporate Disaster While Driving Success*. Wiley.

Tipton, H. (2010) *Information Security Management Handbook*. 4th edn. Auerbach Publications.

Web

www.bcs.org	BCS, The Chartered Institute for IT (General Reference)
www.bsa.org	Software Alliance (General Reference)
www.fast.org.uk	Federation Against Software Theft (General Reference)
www.ico.org.uk	Information Commissioners Office (General Reference)

Links

This unit links to the following related units:

Unit 29: Network Security

Unit 30: Applied Cryptography in the Cloud

Unit 31: Forensics

Unit 32: Information Security Management.

Unit 6: Planning a Computing Project (Pearson-set)

Unit code	**H/618/7407**
Unit type	**Core**
Unit level	**4**
Credit value	**15**

Introduction

This unit is assessed through a Pearson-set assignment. The project brief will be set by the centre, based on a theme provided by Pearson (this will change annually). The theme and chosen project within the theme will enable students to explore and examine a relevant and current topical aspect of computing in the context of a business environment.

As computing systems and technologies continually develop so do the ways in which businesses utilise technologies to support their operations and remain competitive. As a computing professional it is important to understand the ways in which technology evolves and how it can be utilised in different sectors.

The aim of this unit is to give students an opportunity to demonstrate the research skills required for developing a deeper understanding of a subject and the ability to use evidence to inform decisions. Students will undertake independent research, and investigation of a theme set by Pearson. Students will also investigate and research an industry sector as outlined in the centre-set project brief. Students will use the outcomes of their research to help them plan a computer-based project and to support recommendations for how the identified business could utilise the tools and technologies identified as part of their research.

On successful completion of this unit, students will have the confidence to engage in decision making, problem solving, research activities and project planning tasks. They will have the fundamental knowledge and skills that will enable them to investigate and examine relevant computing concepts in a work-related context, determine appropriate outcomes, decisions or solutions and present evidence to various stakeholders in an acceptable and understandable format.

Learning Outcomes

By the end of this unit students will be able to:

LO1 Conduct small-scale research, information gathering and data collection to generate knowledge on an identified subject

LO2 Explore the features and business requirements of organisations in an identified sector.

LO3 Produce project plans based on research of the chosen theme for an identified organisation

LO4 Present your project recommendations and justifications of decisions made, based on research of the identified theme and sector.

Essential Content

LO1 Conduct small-scale research, information gathering and data collection to generate knowledge on an identified subject

Project execution phase:

Selecting appropriate methods of information gathering, data collection and material resourcing.

The distinct phases that support a coherent and logical argument. Use of secondary research to inform a primary empirical study.

Qualitative and quantitative research methods.

Field work:

Selecting a sample of the consumer market, businesses or individuals (those who meet certain characteristics relevant to the research theme) used to gather data (qualitative or quantitative).

Sampling approaches and techniques, including probability and non-probability sampling.

Analysing information and data:

Using data collection tools, such as interviews and questionnaires, and their advantages and disadvantages.

Using analytical techniques such as trend analysis, coding and typologies.

Sources of, and access to, data, including open and public data, administrative and sensitive data, research data.

The principles of data to govern data, including data has value, data should be reusable, data is managed according to its value, data should be fit for purpose.

Ethics, reliability and validity:

Ensure that all research is conducted, data stored, processed and used in an ethical way.

Research should also be reliable (similar results achieved from a similar sample) and valid (the research should measure what it aimed to measure).

Ensure validity and reliability of secondary data and information used, including consideration of who wrote or collected the information or data, age of data collected, original purpose of the data collection, potential errors or variability in the data, potential bias, e.g. sample size, sample participants, questions used, interpretation of results.

LO2 **Explore the features and business requirements of organisations in an identified sector**

Features of businesses:

Types of business, their ownership and liability.

Private, e.g. sole trader, private limited company, public limited company.

Public, e.g. government department, not-for-profit, e.g. charity, voluntary.

Industry sectors, including primary, secondary, tertiary, quaternary.

How an organisation may provide a specific product(s) or service within a sector.

How some organisations provide both products and services.

The concept of diversification to aid business success.

Operational areas of businesses:

The operational areas of a business ('business functions') and how they support the organisation's purpose, e.g. human resources, research and development, sales, marketing, purchasing, production and quality, finance, customer service, IT, administration.

Stakeholders:

Internal stakeholders, e.g. management, employees, shareholders.

External stakeholders, e.g. suppliers, customers, government agencies, communities.

How stakeholders influence business processes and decisions.

The impact of stakeholders on an organisation's success.

Challenges to the success of a business:

Legislation and industry standards relevant to the organisation and sector.

Change management, including planned change, e.g. expansion, diversification, changes in legislation, system upgrades.

Unplanned change, e.g. response to a security breach, disaster response and recovery.

Communication of need for change to stakeholders.

Management of stakeholders before during and after change, e.g. training, target setting, support

Method of implementation of change, e.g. parallel running, direct change over, phased changeover.

Documenting the change process, testing changes to the system and business.

Security and privacy concerns relevant to the organisation and sector.

LO3 **Produce project plans based on research of the chosen theme for an identified organisation**

Project planning and initiation:

The role of a business or systems analyst and the activities they undertake as part of initiation of a project.

Analysing the features and requirements of an identified organisation to establish their requirements.

Recommend potential solutions to identified business needs, including carrying out a cost/benefit analysis, defining business objectives, scope and purpose of the project.

Comprehensive project plans, including defining functional and non-functional requirements of the system, stakeholder requirements and expectations, carrying out impact analysis, prioritising requirements, describing the deliverables to be produced, timescales and time management, costs, change management planning, risk and challenges analysis.

Success criteria to be used, e.g. Key Performance Indicators (KPIs), performance metrics, quality metrics, and business targets.

Use of an identified project management methodology, e.g. Waterfall, Agile, Rapid Application Development (RAD).

Consider approaches to continuous integration, version and source control.

Tools:

Tools for effective project planning, resource planning and allocation, and work breakdown structure, including Project Initiation Documents (PID), bar and Gantt charts, Critical Path Analysis (CPA), risk matrix.

LO4 **Present your project recommendations and justifications of decisions made based on research of the identified theme and sector**

Presenting and communicating project recommendations:

Presenting to different technical and non-technical stakeholders, e.g. emphasis on operational or strategic information, technical terminology used, levels of detail given and simplifying concepts.

Consider the methods and mediums to be used, including written or verbal, report, online or presentation.

Understand how project research and intended audience will influence on method and medium.

Justification of decisions made:

Justification of recommendations, including use of key points from cost/benefit analysis, deliverables, success criteria, impact analysis.

Justifications of planning, including chosen development methodology, work and resource allocation, key deadlines and timescales.

Rationale for decisions made in the recommended solution and project plan, including use of research and data for the identified technology and business sector, analysis of evidence and business requirements, contextual factors specific to the identified organisation.

Reflection on the quality of research:

Quality of secondary and primary data used to inform planning and make decisions.

Awareness that some studies may result in generalised findings and how this can impact on the quality of decisions and the accuracy of conclusions made.

Evaluate the quality of the data and information used to inform project initiation plans, e.g. sample size, sample characteristics, user experience during collection, domain context.

Reach conclusions as to the likely accuracy and reliability of assertions made.

Learning Outcomes and Assessment Criteria

Pass	Merit	Distinction
LO1 Conduct small-scale research, information gathering and data collection to generate knowledge on an identified subject		
P1 Demonstrate qualitative and quantitative research methods to generate relevant primary data for an identified theme. **P2** Examine secondary sources to collect relevant secondary data and information for an identified theme.	**M1** Analyse data and information from primary and secondary sources to generate knowledge on an identified theme.	**D1** Interpret findings to generate knowledge on how the research theme supports business requirements in the identified sector.
LO2 Explore the features and business requirements of organisations in an identified sector		
P3 Discuss the features and operational areas of a businesses in an identified sector. **P4** Discuss the role of stakeholders and their impact on the success of a business.	**M2** Analyse the challenges to the success of a business in an identified sector.	

Pass	Merit	Distinction
LO3 Produce project plans based on research of the chosen theme for an identified organisation		**D2** Evaluate the project planning recommendations made in relation to the needs of the identified organisation and the accuracy and reliability of the research carried out.
P5 Devise comprehensive project plans for a chosen scenario, including a work and resource allocation breakdown using appropriate tools.	**M3** Produce comprehensive project plans that effectively consider aims, objectives and risks/benefits for an identified organization.	
LO4 Present your project recommendations and justifications of decisions made, based on research of the identified theme and sector		
P6 Communicate appropriate project recommendations for technical and non-technical audiences. **P7** Present arguments for the planning decisions made when developing the project plans. **P8** Discuss accuracy and reliability of the different research methods applied.	**M4** Assess the extent to which the project recommendations meet the needs of the identified organisation, including fully-supported rationales for planning decisions made.	

Recommended Resources

Textbooks

Costley, C., Elliot, G. and Gibbs, P. (2010) *Doing Work Based Research: Approaches to Enquiry for Insider-researchers*. London: SAGE.

Dawson, C. (2016) *Projects in Computing and Information Systems: A Student's Guide.* UK: Pearson Education.

Flick, U. (2011) *Introducing Research Methodology: A Beginner's Guide to Doing a Research Project*. London: SAGE.

Gray, D. (2009) *Doing Research in the Real World.* 2nd edn. London: SAGE.

Guay, M., Schreiber, D. and Briones, S. (2016) *The Ultimate Guide to Project Management: Learn everything you need to successfully manage projects and get them done.* Free Kindle Edition. US: Zapier Inc.

Lock, D. (2013) *Project Management 8th* edn. UK: Routledge.

Pinto, J. K. (2015) *Project Management: Achieving Competitive Advantage* 4th edn. Pearson.

Journals

International Journal of Quantitative and Qualitative Research (IJQQRM) – EA Journala

Qualitative Research Journal (QRJ) – Sage Journals

Web

www.apm.org.uk	Association for Project Management (General Reference)
www.gov.uk/government/publications	Department of Business Innovations and Skills, *Guidelines for managing projects – How to organise, plan and control projects*. (Report)
www.hesa.ac.uk	Higher Education Statistics Agency (HESA) – data collection and analysis for higher education
www.ons.gov.uk	Office for National Statistics (ONS) (General Reference)
www.pmi.org.uk	Project Management Institute UK (General Reference)

Links

This unit links to the following related units:

Unit 3: Professional Practice

Unit 16: Computing Research Project (Pearson-set)

Unit 17: Business Process Support

Unit 35: Systems Analysis & Design.

Unit 10: Cyber Security

Unit code	**M/618/5661**
Unit type	**Core**
Unit level	**4**
Credit value	**15**

Introduction

Digital technologies provide an opportunity for malicious hackers and cyberterrorists to exploit individuals, government, institutions and large organisation. Defending against cyber-attacks including insider threats is a priority within the digital technologies sector. Cybercrime techniques and attack vectors are fast-growing taking advantage of the speed, anonymity and convenience of the internet as a facilitator for malicious and criminal activity.

This unit has been designed to develop students' knowledge and understanding in relation to cyber threats and vulnerabilities, cyber defence techniques and incident response. Students will explore fundamental principles as well as leading-edge concepts, terminologies, models, and hardening methods. Students will assess the types of malicious activity and potential targets, and the role everyone has for maintaining cyber resilience.

On successful completion of the unit, students will have explored the nature of cybercrime and cyber threat actors; looked into the roles and responsibilities in relation to information assurance; assessed the threats to, and vulnerabilities in, ICT infrastructure; and investigated strategic responses to cyber security threats.

Learning Outcomes

By the end of this unit, students will be able to:

LO1 Explore the nature of cybercrime and cyber threat actors

LO2 Investigate cyber security threats and hazards

LO3 Examine the effectiveness of information assurance concepts applied to ICT infrastructure

LO4 Investigate incident response methods to cyber security threats.

Essential Content

LO1 Explore the nature of cybercrime and cyber threat actors

Cyber security – the importance to business and society:

Business and society reliance on technology.

Why technology is a target for cybercrime.

Use of technology in business and society, e.g. email correspondence, financial transactions, networking, collaborative work documents, global modes/means of communication.

Impact of cyber security on protecting business and society.

Risks of not educating end users in security measures with regular updates to users.

Key definitions:

Cybercrime, cyber security, malicious cyber activity, hacker, malware, phishing, cyber resilience.

Cyber threat actors:

For example, cyber terrorists, government-sponsored/state-sponsored actors, organised crime/cybercriminals, 'hacktivists', insiders, internal user errors.

Targets:

For example, critical national infrastructure, mainframes, data centres, mobile phones, consumers, individuals, business, websites.

The categorisation of activity:

Active attacks attempt to alter system resources.

Passive attacks, attempts to learn or make use of information from the system without affecting the integrity of targeted systems, e.g. wiretapping.

Attacks can be initiated from inside or outside the perimeters.

Digital systems as 'target', e.g. viruses, attacks against hardware and software, malware, ransomware, hacking, distributed denial of service attacks, e.g. malware, mail bombing, pagejacking

Digital systems as a 'tool', e.g. cyber-enabled crimes, crimes against children, financial crimes, e.g. fraud, identity theft, information warfare, phishing, spam, propagation of obscene or offensive content.

LO2 **Investigate cyber security threats and hazards**

Threats and hazards:

Types of threats and hazards to a system, service, process, e.g. cybercriminals, organised crime groups, states and state-sponsored activity, terrorists, 'hacktivists', script kiddies, insiders (knowing and accidental).

Threat behaviour.

Missing data encryption.

Global threat landscape.

Individual and business fraud, extortion, trolling, racketeering, 'black market' sales, embezzlement, cyberstalking, cyber terrorism, industrial espionage, prostitution, gambling, suicide assistance.

Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks.

Man-in-the-middle (MitM) attacks.

Phishing and spear phishing attacks.

Drive-by attacks.

Password attacks; brute-force, factionary etc.

SQL injection attacks.

Cross-site scripting (XSS) attacks.

Eavesdropping attacks.

Advanced Persistent Threats (APTs).

Hazards and sources of potential damage, harm, adverse effect, e.g. life, political, military, organisational, critical infrastructure, economy, social group, technology, environmental, legal.

Cyber threat intelligence (CTI):

Importance of threat intelligence.

CTI types, including tactical, operational, strategic.

Evidence-based CTI.

Attribution and signs of accountability.

Risk of not acting on intelligence.

Acting on threat intelligence.

Emerging threats:

Horizon scanning, e.g. increased dependency on technology, increased use of robots, quantum technologies, low-orbiting satellites, Internet of Things (IoT), increased threats from developing countries as computer literacy increases.

LO3 **Examine the effectiveness of information assurance concepts applied to ICT infrastructure**

Information assurance and governance concepts:

Assurance, trustworthy vs trusted, user awareness of security requirements.

Achieving assurance in practice, e.g. penetration testing and contribution to assurance, extrinsic assurance methods.

Definitions and Information Architecture (IA) principles, data, information and IT governance, Information Governance (IG) roles and responsibilities.

Accountability, legal and regulatory applicability and requirements.

Recovery, IG strategic planning and best practices, IG policy development, IG business consideration and legal functions.

IG standardisation and accepted practices, IG auditing and enforcement, monitoring.

Records management and inventorying, IT and data governance frameworks.

IG in the cloud, social media and mobile devices, maintain an IG programme (challenges and opportunities).

ICT infrastructure:

ICT infrastructure, e.g. fundamental building blocks and typical architectures.

Common vulnerabilities in networks and systems.

Hardware, storage, routers/switches, application software, operating systems.

Traditional, cloud or hyper converged IT Infrastructure.

IoT, IIoT and IoMT.

LO4 **Investigate incident response methods to cyber security threats**

Standards:

International Organization for Standardisation (ISO) e.g. ISO/IEC 27001 Information Security Management, ISO/IEC 27002:2013.

Information technology security techniques, code of practice for information security controls.

Encryption standards, including AES – Advanced Encryption Standard, RSA – Rivest Shamir Adleman, 3DEA – Triple Data Encryption Algorithm, PGP – Pretty Good Privacy, common international encryption laws and policies, e.g. General Right of Encryption, Mandatory Minimum or Maximum Encryption Strength, Licensing/Regulation Requirements, Import/Export Controls, Obligations on Providers to Assist Authorities, Obligations on Individuals to Assist Authorities.

Legislation:

UK specific laws and policies, e.g. Electronic Communications Act (2000), Electronic Signatures Regulations (2002), Wassenaar Arrangement (1996), Regulation of Investigatory Powers Act (2016), International Traffic in Arms Regulations (ITAR), disclosure laws, e.g. Public Interest Disclosure Act (1998), Freedom of Information Act (2000), Data Protection Act (2018), General Data Protection Regulation (GDPR) (2016), Computer Misuse Act (1990), The Serious Crime Act (2015), Police and Justice Act (2006), Terrorism Act (2000), Human Rights Act (1998), Digital Economy Act (2017), Extradition Act (2003), Crime and Courts Act (2013) (to prevent extradition), Interception of Communication Act (1985).

Incident response methodology:

Preparation, Detection and Analysis, Containment, Eradication, and Recovery.

Developing a containment strategy, identifying and mitigating the hosts and systems under attack, and having a plan for recovery.

Post-incident activity.

The principles and elements of incident management.

Guidelines for incident responders and computer forensic investigations, together with legal aspects and relevant laws.

Intrusion detection and response methods.

Cryptography:

Contemporary use of cryptography, e.g. data encryption in storage, in usage and in transit (disks, network), data hashing (verification of origin, passwords, look-up tables, software verification, MD5).

Future trends in cryptography, e.g. blowfish, twofish, honey encryption, quantum key distribution.

Asymmetric and symmetric cryptography.

Organisations:

Organisations involved in preventing cyber security threats, e.g. National Cyber Security Centre (NCSC), police, National Crime Agency (NCA), National Cybercrime Unit (NCCU), Military Cyber Security Operations Centre (MCSOC), Regional Organised Crime Units (ROCUs).

Learning Outcomes and Assessment Criteria

<table>
<tr><th>Pass</th><th>Merit</th><th>Distinction</th></tr>
<tr><td colspan="2">LO1 Explore the nature of cybercrime and cyber threat actors</td><td rowspan="5">D1 Evaluate types of malicious cyber activity and the action that can be taken to neutralise cyber threat actors.</td></tr>
<tr><td>P1 Review types of malicious and/or criminal cyber activity.
P2 Investigate the potential targets of cybercrime.</td><td>M1 Analyse the concept of digital systems as ‘targets’ and ‘tools’ as related to cyber security, giving real-world examples.</td></tr>
<tr><td colspan="2">LO2 Investigate cyber security threats and hazards</td></tr>
<tr><td>P3 Describe security threats and hazards to a system or service or process.
P4 Investigate common attack techniques and recommend how to defend against them.</td><td>M2 Assess the role of threat intelligence when defending against common attack techniques.</td></tr>
<tr><td colspan="2">LO3 Examine the effectiveness of information assurance concepts applied to ICT infrastructure</td></tr>
<tr><td>P5 Explore how information assurance concepts can mitigate threats and vulnerabilities in ICT infrastructure, giving examples.</td><td>M3 Assess how information assurance could enhance the cyber resilience of ICT infrastructure.</td><td rowspan="3">D2 Evaluate the responses that have been implemented by different organisations in response to cyber security threats.</td></tr>
<tr><td colspan="2">LO4 Investigate incident response methods to cyber security threats</td></tr>
<tr><td>P6 Describe security standards, regulations and their consequences across at least two sectors.
P7 Investigate the types of response that have been implemented in response to cyber security threats.</td><td>M4 Analyse the role of criminal and other law in deterring cybercrime.</td></tr>
</table>

Recommended resources

Textbooks

Amoroso, E. and Amoroso, M. (2017) *From CIA to APT: An Introduction to Cyber Security.* New York: Independently published.

Gillespie, A. A. (2015) *Cybercrime.* Oxon: Routledge.

GRABOSKY, P. (2015) *Cybercrime (Keynotes Criminology & Criminal Justice).* New York: Oxford University Press.

Stevens, T. (2015) *Cyber Security and the Politics of Time.* Cambridge: Cambridge University Press.

Sutton, D. (2017) Cyber Security: A practitioner's guide. Swindon: BCS, The Chartered Institute for IT.

Web

interpol.int	Interpol crime areas, cybercrime (General Reference)
nationalcrimeagency.gov.uk	National Crime Agency – crime threats, cybercrime (General Reference)
ncsc.gov.uk	National Cyber Security Centre (General Reference)

Links

This unit links to the following related units:

Unit 5: Security

Unit 30: Applied Cryptography in the Cloud.

Unit 14: Maths for Computing

Unit code	**R/618/7421**
Unit level	**4**
Credit value	**15**

Introduction

In 1837, English mathematicians Charles Babbage and Ada Lovelace in collaboration, described a machine that could perform arithmetical operations and store data in memory units. This design of their 'Analytical Engine' is the first representation of modern, general-purpose computer technology. Although modern computers have advanced far beyond Babbage and Lovelace's initial proposal, they still rely fundamentally on mathematics for their design and operation.

This unit introduces students to the mathematical principles and theory that underpin the computing curriculum. Through a series of case studies, scenarios and task-based assessments, students will explore number theory in a variety of scenarios; use applicable probability theory; apply geometrical and vector methodology; and, finally, evaluate problems concerning differential and integral calculus.

Among the topics included in this unit are: prime number theory, sequences and series, probability theory, geometry, differential calculus and integral calculus.

On successful completion of this unit, students will have gained confidence in the mathematics that is needed in other computing units. They will have developed skills such as communication literacy, critical thinking, analysis, reasoning and interpretation, which are crucial for gaining employment and developing academic competence.

Learning Outcomes

By the end of this unit students will be able to:

LO1 Use applied number theory in practical computing scenarios

LO2 Analyse events using probability theory and probability distributions

LO3 Determine solutions of graphical examples using geometry and vector methods

LO4 Evaluate problems concerning differential and integral calculus.

Essential Content

LO1 Use applied number theory in practical computing scenarios

Number theory:

Converting between number bases (denary, binary, octal, duodecimal and hexadecimal).

Prime numbers, Pythagorean triples and Mersenne primes. Greatest common divisors and least common multiples.

Modular arithmetic operations.

Sequences and series:

Expressing a sequence recursively.

Arithmetic and geometric progression theory and application. Summation of series and the sum to infinity.

LO2 Analyse events using probability theory and probability distributions

Probability theory:

Calculating conditional probability from independent trials. Random variables and the expectation of events.

Applying probability calculations to hashing and load balancing.

Probability distributions:

Discrete probability distribution of the binomial distribution.

Continuous probability distribution of the normal (Gaussian) distribution.

LO3 Determine solutions of graphical examples using geometry and vector methods

Geometry:

Cartesian co-ordinate systems in two dimensions. Representing lines and simple shapes using co-ordinates. The co-ordinate system used in programming output device.

Vectors:

Introducing vector concepts.

Cartesian and polar representations of a vector. Scaling shapes described by vector co-ordinates.

LO4 **Evaluate problems concerning differential and integral calculus**

Differential calculus:

Introduction to methods for differentiating mathematical functions. The use of stationary points to determine maxima and minima.

Using differentiation to assess rate of change in a quantity.

Integral calculus:

Introducing definite and indefinite integration for known functions. Using integration to determine the area under a curve.

Formulating models of exponential growth and decay using integration methods.

Learning Outcomes and Assessment Criteria

Pass	Merit	Distinction
LO1 Use applied number theory in practical computing scenarios		
P1 Calculate the greatest common divisor and least common multiple of a given pair of numbers. **P2** Use relevant theory to sum arithmetic and geometric progressions.	**M1** Identify multiplicative inverses in modular arithmetic.	**D1** Produce a detailed written explanation of the importance of prime numbers in the field of computing.
LO2 Analyse events using probability theory and probability distributions		
P3 Deduce the conditional probability of different events occurring in independent trials. **P4** Identify the expectation of an event occurring from a discrete, random variable.	**M2** Calculate probabilities in both binomially distributed and normally distributed random variables.	**D2** Evaluate probability theory to an example involving hashing and load balancing.
LO3 Determine solutions of graphical examples using geometry and vector methods		
P5 Identify simple shapes using co-ordinate geometry. **P6** Determine shape parameters using appropriate vector methods.	**M3** Evaluate the co-ordinate system used in programming a simple output device.	**D3** Construct the scaling of simple shapes that are described by vector co-ordinates.

Pass	Merit	Distinction
LO4 Evaluate problems concerning differential and integral calculus		
P7 Determine the rate of change in an algebraic function. **P8** Use integral calculus to solve practical problems involving area.	**M4** Analyse maxima and minima of increasing and decreasing functions, using higher order derivatives.	**D4** Justify, by further differentiation, that a value is a minimum.

Recommended Resources

Textbook

Stroud, K. A. (2009) *Foundation Mathematics*. Basingstoke: Palgrave Macmillan.

Journal

Journal of Computational Mathematics. Global Science Press.

Links

This unit links to the following related units:

Unit 18: Discrete Maths

Unit 33: Applied Analytical Models.

Unit 16: Computing Research Project (Pearson-set)

Unit code	**K/618/7425**
Unit type	**Core**
Unit level	**5**
Credit value	**30**

Introduction

This unit is assessed through a Pearson-set assignment. Students will choose their own project based on a theme provided by Pearson (this will change annually). The project must be related to their specialist pathway of study (unless the student is studying the general computing pathway). This will enable students to explore and examine a relevant and current topical aspect of computing in the context of a business environment and their chosen specialist pathway.

The aim of this unit is to give students the opportunity to engage in sustained research in a specific field of study. Students will be able to demonstrate the capacity and ability to identify a research theme, to develop research aims, objectives and outcomes, and to present the outcomes of such research in both written and verbal formats. Students are encouraged to reflect on their engagement in the research process, during which recommendations for personal development are key learning points.

On successful completion of this unit, students will have the confidence to engage in problem-solving and research activities. Students will have fundamental knowledge and skills that will enable them to investigate workplace issues and problems, determine appropriate solutions and present evidence to various stakeholders in an acceptable and understandable format.

Students will have developed skills such as communication literacy, critical thinking, analysis, synthesis, reasoning, and interpretation, which are crucial for gaining employment and developing academic competence.

Learning Outcomes

By the end of this unit students will be able to:

LO1 Examine appropriate research methodologies and approaches as part of the research process

LO2 Conduct and analyse research relevant to a computing research project

LO3 Communicate the outcomes of a research project to identified stakeholders

LO4 Reflect on the application of research methodologies and concepts.

Essential Content

LO1 Examine appropriate research methodologies and approaches as part of the research process

Developing a research proposition:

The importance of developing methodical and valid propositions as the foundation for a research project.

Rationale: the purpose and significance for research question or hypothesis.

The value of the philosophical position of the researcher and the chosen methods.

Use of Saunders' Research Onion as a guide to establishing a methodological approach.

Literature review:

Conceptualisation of the research problem or hypothesis.

The importance of positioning a research project in context of existing knowledge.

Significance and means of providing benchmarks by which data can be judged.

Qualitative, quantitative, and mixed method research methodologies:

Key theoretical frameworks for research.

Advantages and limitations of qualitative and quantitative research approaches and methods.

LO2 Conduct and analyse research relevant to a computing research project

Research as a process:

Follow distinct phases of research to support a coherent and logical argument including using secondary research to inform a primary, empirical study.

Identify the reason and goal of the business research project, e.g. solving identified problems, business expansion, improve competitiveness, response to developments in technology, changes in the industry.

Elicite information from stakeholders.

Application of key skills and behaviours to guide the research project and ensure success, e.g. critical thinking, analysis and reasoning, dealing with difficult situations, misunderstanding or mistakes.

Selecting a sample:

The importance of gathering primary and secondary data and information (qualitative or quantitative) to support research analysis.

Selecting sample types and sizes that are relevant to the research.

Considering sampling approaches and techniques, including probability and non-probability (random) sampling.

Ethics, reliability and validity:

Conduct research ethically including reporting of findings.

Consider how to ensure reliable and valid research.

Analysing data:

Using data collection tools such as interviews and questionnaires.

Using analytical techniques such as trend analysis, coding and typologies.

LO3 **Communicate the outcomes of a research project to identified stakeholders**

Stakeholders:

Techniques to support the identification and analysis of internal and external stakeholders.

Stakeholder analysis to determine approaches to communications, including who the stakeholders are, high and low priority status, type of communication, frequency of communication, level to which the project outcomes are conveyed.

Communicating research outcomes:

Consideration of different methods of communicating outcomes, e.g. written word, spoken word, and the medium, e.g. report, online, presentation. The method and medium will be influenced by the research and its intended audience.

Considerations when communicating with stakeholders, e.g. maintaining privacy and security, tone of voice, use of technical vocabulary or jargon, maintaining or promoting company image.

Convincing arguments:

No matter what the method/medium, all research should be convincing and presented logically where the assumption is that the audience has little or no knowledge of the research process.

The importance of developing evaluative conclusions.

LO4 **Reflect on the application of research methodologies and concepts**

Reflection for learning and practice:

Difference between reflecting on performance and evaluating a research project. The former considers the research process; the latter considers the quality of the research argument and use of evidence.

Reflection on the merits, limitations and potential pitfalls of the chosen methods.

The cycle of reflection:

To include reflection in action and reflection on action.

Considering how to use reflection to inform future behaviour and future considerations.

Reflective writing:

Avoiding generalisation and focusing on personal development and the research journey in a critical and objective way.

Learning Outcomes and Assessment Criteria

<table>
<tr><th>Pass</th><th>Merit</th><th>Distinction</th></tr>
<tr><td colspan="2">LO1 Examine appropriate research methodologies and approaches as part of the research process</td><td rowspan="5">D1 Critically evaluate research methodologies and processes in application to a computing research project to justify chosen research methods and analysis.</td></tr>
<tr><td>P1 Produce a research proposal that clearly defines a research question or hypothesis, supported by a literature review.

P2 Examine appropriate research methods and approaches to primary and secondary research.</td><td>M1 Analyse different research approaches and methodology and make justifications for the choice of methods selected based on philosophical/theoretical frameworks.</td></tr>
<tr><td colspan="2">LO2 Conduct and analyse research relevant to a computing research project</td></tr>
<tr><td>P3 Conduct primary and secondary research using appropriate methods for a computing research project that consider costs, access and ethical issues.

P4 Apply appropriate analytical tools, analyse research findings and data.</td><td>M2 Discuss merits, limitations and pitfalls of approaches to data collection and analysis.</td></tr>
</table>

Pass	Merit	Distinction
LO3 Communicate the outcomes of a research project to identified stakeholders		
P5 Communicate research outcomes in an appropriate manner for the intended audience.	**M3** Analyse the extent to which outcomes meet set research objectives and communicate judgements effectively for the intended audience	**D2** Evaluate outcomes and make valid, justified recommendations.
LO4 Reflect on the application of research methodologies and concepts		
P6 Discuss the effectiveness of research methods applied, for meeting objectives of the computing research project. **P7** Discuss alternative research methodologies and lessons learnt in view of the outcomes.	**M4** Analyse results in recommended actions for improvements and future research considerations.	**D3** Demonstrate reflection and engagement in the resource process, leading to recommended actions for future improvement.

Recommended Resources

Textbooks

Cornford, T., Smithson S. (2005) *Project Research in Information Systems: A Student's Guide*. Paperback. Palgrave Macmillan.

Costley, C., Elliott, G. and Gibbs, P. (2010) *Doing Work Based Research: Approaches to Enquiry for Insider-researchers.* London: SAGE.

Fink, A. (2020) *Conducting Research Literature Reviews: From the Internet to Paper*. 5th edn. Sage Publications Inc.

Flick, U. (2020) *Introducing Research Methodology: A Beginner's Guide to Doing a Research Project.* London: Sage Publications Ltd.

Gray, D.E. (2009) *Doing Research in the Real World.* 2nd edn. London: SAGE.

Saunders, M., Lewis, P. and Thornhill, A. (2012) *Research Methods for Business Students.* 6th edn. Harlow: Pearson.

Wellington, J. (2000) *Educational Research: Contemporary Issues and Practical Approaches*. Continuum International Publishing Group Ltd.

Journals

International Journal of Quantitative and Qualitative Research

Qualitative Research

Links

This unit links to the following related units:

Unit 3: Professional Practice

Unit 6: Planning a Computing Project (Pearson-set)

Unit 7: Software Development Lifecycles.

Unit 17: Business Process Support

Unit code	**A/618/7428**
Unit type	**Core**
Unit level	**5**
Credit value	**15**

Introduction

Data and information are core to any organisation and business process. Accurate data and meaningful information are of high value to an organisation and are key drivers for effective decision making and problem solving. Business intelligence relies on the use of data science, which makes use of a range of tools and methods, including data mining, data integration, data quality and data warehousing, in conjunction with other information management systems and applications.

This unit introduces students to a range of tools, techniques and technologies used for acquiring data and processing it into meaningful information that can be used to support business functions and processes.

Students will examine how data and information support business processes, the mechanisms to source and utilise data and turn it in to usable, and valuable, information output. Students will explore real-world business problems, the emergence of data science and how the application of data science can be used to support business processes. Finally, students will demonstrate practical application of data science techniques to support real-world business problems.

On successful completion of this unit, students will appreciate the importance and value of data and information in terms of optimising decision making and performance. By exploring the tools, techniques and systems that support business processes, students will be aware of the role and contribution of these technologies and methodologies, and their importance to organisations. As a result, students will develop skills such as communication literacy, critical thinking, analysis, reasoning and interpretation, which are crucial for gaining employment and developing academic competence.

Learning Outcomes

By the end of this unit students will be able to:

LO1 Discuss the use of data and information to support business processes and the value they have for an identified organisation

LO2 Discuss the implications of the use of data and information to support business processes in a real-world scenario

LO3 Explore the tools and technologies associated with data science and how it supports business processes

LO4 Demonstrate the use of data science techniques to make recommendations to support real-world business problems.

Essential Content

LO1 **Discuss the use of data and information to support business processes and the value they have for an identified organisation**

Data and information in organisations:

Value of data and information for an organisation, including decision making (strategic, tactical and operational), deliver and improve services, optimise workflow and efficiency, increase profit margins, diversification, reduce overheads.

Types of data used by organisations, including structured and unstructured data.

Impact on business processes in terms of elicitation and storage.

The importance of reliable data and impact on businesses.

Use of data and information to support business processes:

Analysing market trends to identify patterns.

Factors impacting fluctuations in supply and demand, and prices of goods.

Monitoring system performance metrics.

Monitoring and controlling the quality of a product or service.

Analysing levels of user or customer interaction and engagement.

Analysing trends in browsing and purchasing for targeted marketing purposes.

Mechanisms:

Data generation, including human generated, e.g. social media posts, documents and files, email and text messages, website content.

Machine generated data, e.g. sensor readings, log files, system performance metrics, transactional data.

Tools to collect, store, manage, analyse and display data and information, including application software, content management systems, social media platform analytics tools, databases, scripting languages.

LO2 **Discuss the implications of the use of data and information to support business processes in a real-world scenario**

Social, legal and ethical implications:

Recognise the social, ethical and professional issues related to the use of data and information to support business processes, e.g. how data and information is collected and used, use of cookies and other transactional data, sharing of data, e.g. between departments, services and organisations.

Legal and regulatory issues related to the use of data and information to support business processes in reference to current legislation and principles of good practice, as recommended by computing professional bodies.

Cybersecurity management:

Common threats to data and information, e.g. internal and external threats.

Impact of human behaviour on cyber security, e.g. how motive and opportunity combine to become a threat.

Concept of 'secure by design' when developing and using systems to handle data and information.

Ways to mitigate common threats to data and information at personal and organisational level.

Organisational implications of failing to adequately protect data and information, e.g. legal actions, financial impact, disruption of operations and reduction in productivity, damage to public image.

LO3 **Explore the tools and technologies associated with data science and how it supports business processes**

Data science overview:

Explore how the exponential growth of the amount of data generated impacts on the way data is collected and used.

The core aims of data science, including making data useful and retrievable, extracting actionable intelligence to improve business performance, automating extraction and implementation.

Key job roles, including data engineer and data scientist, and how they work with other members of a team, e.g. senior managers, business and data analysts, software engineers in change and development lifecycles.

Data-science-related skills, including mathematics and statistics, programming and scripting skills, investigation and integration of data, core business knowledge.

Sub-disciplines in the data science field, including data engineering, machine learning and artificial intelligence.

Using data:

Core data handling techniques and concepts, including input and capture, data processing and conversion, information output and security considerations.

Forms of data, including unstructured and semi-structured data, and implications on use and analysis.

Data types, e.g. date, integer, real, character, string, Boolean.

Format of source and target data files, e.g. JSON, fixed-width text file, CSV, ASCII, XML.

The use of coding and scripting languages to automate data science processes, e.g. Python, R.

Turning data into usable information, including data mining techniques to find anomalies, cluster patterns and relationships between data sets, web scraping, descriptive and predictive analysis, converting data into visual information, e.g. charts, graphs, histograms, other visual mediums.

Predictive modelling, e.g. forecasting, use of statistical models to predict and identify trends.

Communicating information effectively to a range of stakeholders.

LO4 **Demonstrate the use of data science techniques to make recommendations to support real-world business problems**

Solutions:

Supporting a business process, including techniques to elicit end user requirements, systems requirements, application to automate procedures, including when it is most appropriate to use each one.

Designing a tool, program or package that can perform a specific task to support problem solving or decision making, e.g. e-commerce function for a website to support purchase analysis, a user dashboard to investigate specific market trends, optimising delivery routes for a logistics company.

Analysing and modelling business processes using relevant techniques, standards, notation and software tools.

Design considerations:

Addressing user and system requirements, e.g. user-friendly and functional interface, considering user engagement and interaction, quality risks inherent in data, mitigate or resolve risks, meaningful data output, customisation to satisfy the user and system requirements, phases of testing of business system changes.

Learning Outcomes and Assessment Criteria

<table>
<tr><th>Pass</th><th>Merit</th><th>Distinction</th></tr>
<tr><td colspan="2">LO1 Discuss the use of data and information to support business processes and the value they have for an identified organisation</td><td rowspan="5">D1 Evaluate the wider implications of using data and information to support business processes in an identified organisation.</td></tr>
<tr><td>P1 Discuss how data and information support business processes and the value they have for organisations.

P2 Discuss how data is generated and the tools used to manipulate it to form meaningful data to support business operations.</td><td>M1 Assess the value of data and information to individuals and organisations in relation to real-world business processes.</td></tr>
<tr><td colspan="2">LO2 Discuss the implications of the use of data and information to support business processes in a real-world scenario</td></tr>
<tr><td>P3 Discuss the social legal and ethical implications of using data and information to support business processes.

P4 Describe common threats to data and how they can be mitigated at on a personal and organisational level.</td><td>M2 Analyse the impact of using data and information to support business real-world business processes.</td></tr>
</table>

Pass	Merit	Distinction
LO3 Explore the tools and technologies associated with data science and how it supports business processes		
P5 Discuss how tools and technologies associated with data science are used to support business processes and inform decisions.	**M3** Assess the benefits of using data science to solve problems in real-world scenarios.	**D2** Evaluate the use of data science techniques against user and business requirements of an identified organisation.
LO4 Demonstrate the use of data science techniques to make recommendations to support real-world business problems		
P6 Design a data science solution to support decision making related to a real-world problem. **P7** Implement a data science solution to support decision making related to a real-world problem.	**M4** Make justified recommendations that support decision making related to a real-world problem.	

Recommended Resources

Textbooks

Boyer, J. (2010) *Business Intelligence Strategy*. MC Press (US).

Jeston, J. and Nelis, J. (2018) *Business Process Management*. 4th edn. Routledge.

Kolb, J. (2013) *Business Intelligence in Plain Language: A practical guide to Data Mining and Business Analytics*. CreateSpace Independent Publishing Platform.

Marr, B. (2015) *Big Data: Using SMART Big Data, Analytics and Metrics to Make Better Decisions and Improve Performance.* 1st edn. John Wiley & Sons, Ltd.

VanderPlas, J. (2016) *Python Data Science Handbook: Tools and Techniques for Developers: Essential Tools for Working with Data*. O'Reilly.

Journals

International Journal of Business Intelligence and Data Mining

International Journal of Business Intelligence Research (IJBIR)

Web

gartner.com/en	Research and Advisory (General Reference)
datascience.codata.org	Data science (Online data science journal)

Links

This unit links to the following related units:

Unit 6: Planning a Computing Project (Pearson-set)

Unit 8: Data Analytics

Unit 33: Applied Analytical Models

Unit 34: Analytical Methods.

Unit 18: Discrete Maths

Unit code	**F/618/7429**
Unit level	**5**
Credit value	**15**

Introduction

Digital computer technologies operate with distinct steps and data is stored as separate bits. This method of finite operation is known as 'discrete', and the division of mathematics that describes computer science concepts such as software development, programming languages and cryptography is known as 'discrete mathematics'. This branch of mathematics is a major part of a computer science course and aids, ultimately, in the development of logical thinking and reasoning that lies at the core of all digital technology.

This unit introduces students to the discrete mathematical principles and theory that underpin software engineering. Through a series of case studies, scenarios and task-based assessments, students will explore set theory and functions in a variety of scenarios, perform analysis using graph theory, apply Boolean algebra to applicable scenarios and, finally, explore additional concepts in abstract algebra.

Among the topics included in this unit are set theory and functions, Eulerian and Hamiltonian graphs, binary problems, Boolean equations, algebraic structures and group theory.

On successful completion of this unit, students will have gained confidence in the discrete mathematics that is needed to understand software engineering concepts. As a result, they will have developed skills such as communication literacy, critical thinking, analysis, reasoning and interpretation, which are crucial for gaining employment and developing academic competence.

Learning Outcomes

By the end of this unit students will be able to:

LO1 Examine set theory and functions applicable to software engineering

LO2 Analyse mathematical structures of objects using graph theory

LO3 Investigate solutions to problem situations using the application of Boolean algebra

LO4 Explore applicable concepts within abstract algebra.

Essential Content

LO1 **Examine set theory and functions applicable to software engineering**

Set theory:

Sets and set operations. Algebra within set theory.

Set identities and proof of identities. Bags manipulation functions.

Functions:

Domain, range and mappings.

Inverse relations and the inverse function. Injective and surjective functions, and transitive relations

LO2 **Analyse mathematical structures of objects using graph theory**

Graph theory:

Structure and characterisation of graphs. Spanning trees and rooted trees.

Eulerian and Hamiltonian graphs. Vertex and edge colourings of graphs.

Directed graphs:

Directed and undirected graphs.

Walks, trails, paths and shortest paths.

LO3 **Investigate solutions to problem situations using the application of Boolean algebra**

Boolean algebra:

Binary states (e.g. on/off; 1/0; open/closed; high/low).

Identification of binary problems and labelling inputs and outputs. Production of a truth table corresponding to a problem situation.

Equations:

Express a truth table as a Boolean equation.

Simplify a Boolean equation using algebraic methods. Represent a Boolean equation using logic gates.

LO4 **Explore applicable concepts within abstract algebra**

Algebraic structures:

Binary operations and associated properties. Commutative and associative operations.

Algebraic structures and substructures.

Groups:

Introduction to groups, semigroups and monoids. Families of groups and group codes.

Substructures and morphisms.

Learning Outcomes and Assessment Criteria

Pass	Merit	Distinction
LO1 Examine set theory and functions applicable to software engineering		
P1 Perform algebraic set operations in a formulated mathematical problem. **P2** Determine the cardinality of a given bag (multiset).	**M1** Determine the inverse of a function using appropriate mathematical techniques.	**D1** Formulate corresponding proof principles to prove properties about defined sets.
LO2 Analyse mathematical structures of objects using graph theory		
P3 Model contextualised problems using trees, both quantitatively and qualitatively. **P4** Use Dijkstra's algorithm to find a shortest path spanning tree in a graph.	**M2** Assess whether a Eulerian and Hamiltonian circuit exists in an undirected graph.	**D2** Construct a proof of the Five Color Theorem.

Pass	Merit	Distinction
LO3 Investigate solutions to problem situations using the application of Boolean algebra		
P5 Diagram a binary problem in the application of Boolean algebra. **P6** Produce a truth table and its corresponding Boolean equation from an applicable scenario.	**M3** Simplify a Boolean equation using algebraic methods.	**D3** Design a complex system using logic gates.
LO4 Explore applicable concepts within abstract algebra		
P7 Describe the distinguishing characteristics of different binary operations that are performed on the same set. **P8** Determine the order of a group and the order of a subgroup in given examples.	**M4** Validate whether a given set with a binary operation is indeed a group.	**D4** Explore, with the aid of a prepared presentation, the application of group theory relevant to your given example.

Recommended Resources

Textbooks

Attenborough, M. (2003) *Mathematics for Electrical Engineering and Computing.* Oxford: Newnes.

Piff, M. (2008) *Discrete Maths Software Engineers: An Introduction for Software Engineers.* Cambridge: Cambridge University Press.

Journals

Journal of Graph Theory. Wiley.

Journal of Mathematical Modelling and Algorithms in Operations Research. Springer.

Links

This unit links to the following related units:

Unit 14: Maths for Computing

Unit 33: Applied Analytical Models.

Unit 30: Applied Cryptography in the Cloud

Unit code	**F/618/4899**
Unit level	**5**
Credit value	**15**

Introduction

Almost every interaction we make with an electronic device will involve cryptography in some form. Cryptography is an indispensable tool for protecting information in computer systems. Applied cryptography for cloud services uses encryption techniques that protects data used, shared and stored in the cloud. Cryptography underpins many aspects of security and is a crucial component in protecting the confidentiality and integrity of information. Given the considerable information on individuals and organisations identified in the cloud, concerns are often raised regarding the safety of the cloud environment. Dangers of uploading data into this new environment requires cryptographers and cryptanalysts to protect the cloud environment using a variety of technologies, processes and forms of encryption. The complexity with how cloud computing manages data secrecy and information security is another reason people avoid the cloud. As a result, despite the hype surrounding cloud computing, some users remain reluctant to deploy their personal information or deploy commercial enterprises into the cloud. Understanding cloud security issues, the application of crypto algorithms and to ensure data is secured are vital to its continued functionality, longevity and sustainability. In addition, students are expected to understand the differences between the roles and responsibilities of a cryptographer and cryptanalyst.

This unit introduces students to the applied principles of cryptography and looks at its practical applications and methods, many of which are fundamental to secure data in the cloud. Students are expected to analyse fundamental symmetric, asymmetric and hashing encryption methods, and investigate examples of these in practice. Students are expected to demonstrate the use of cryptography and cryptanalysis tools, methods and their applications. Students are also expected to appraise the inner workings of cryptographic protocols and principles, including transport layer security (TLS) and blockchain, and evaluate how they can be used by organisations to enhance security when considering a move to a cloud environment. Among the topics included in this unit are: the mathematical algorithms used in cryptography, the mechanisms by which cryptographic and cryptanalysis work, hashing and salting, cloud-hosted public key infrastructure (PKI), benefits of encryption techniques, quantum cryptography, secure

multi-party computation, security risks and issues with public key encryption, practical applications of cryptography and Cryptography as a Service (CaaS).

On successful completion of this unit students will be able to analyse functions of stream ciphers and block ciphers, produce code implementing ciphers, analyse methods such as KEM, DEM and PKE's to secure data in a cloud environment. Students will design a security case and implement it demonstrating the use of cryptographic and cryptoanalysis tools for improving security in a virtual private network, for an organisation considering a move to the cloud. As a result, they will develop skills such as critical thinking, analysis, and interpretation, which are crucial for gaining employment and developing academic competence.

Learning Outcomes

By the end of this unit, students will be able to:

LO1 Analyse encryption ciphers and algorithms as methods to secure data in a cloud environment

LO2 Discuss security risks and issues related to public key encryption in practice

LO3 Demonstrate the use of cryptographic and cryptoanalysis tools for improving security in a virtual private network

LO4 Evaluate advanced encryption protocols and their application for an organisation considering a move to the cloud.

Essential Content

LO1 **Analyse encryption ciphers and algorithms as methods to secure data in the cloud environment**

Symmetric Encryption:

Use of ciphers for e.g. secure messages, cloud storage.

Symmetric to include Transposition Cipher, Substitution Cipher, Lorenz Cipher.

Feistel Cipher including Data Encryption Standard (DES).

Triple Data Encryption (3DES).

Rijndael Cipher e.g. Advanced Encryption standard (AES).

Stream cipher (e.g. Rivest Cipher 4).

Block Cipher Mode (e.g. Blowfish, Twofish, Rivest Cipher 5).

Message Authentication Code (MAC).

One-time pad.

Asymmetric Encryption:

Use of algorithms for e.g. authenticity using digital signatures, website security, withdraw or transfer bitcoin.

Asymmetric to include digital signature algorithm (DSA), public key encryption algorithms such as Rivest Shamir Adleman (RSA) algorithm (e.g. RSA cryptosystem), Diffie-Hellman, El Gamal, Elliptic Curve Cryptography (ECC), ECSTR for Efficient and Compact Subgroup Trace (XTR).

Hashing:

Use of hashing for e.g. sharing documents, database encryption, safeguarding passwords.

Hashing to include message digest, secure hashing algorithm. Galois/Counter mode (GCM), MD5, Secure Hash Algorithm 1 (SHA-1), Secure Hash Algorithm 2 (SHA-2), RIPE Message Digest (RIPEMD), homomorphic encryption.

LO2 **Discuss security risks and issues related to public key encryption in practice**

Attacks on public key schemes:

Exploring most common attacks on public key encryption schemes using a range of examples e.g. Wiener's attack on RSA, Lattice-based attacks on RSA, partial key exposure attacks, Meet-in-the-Middle (MITM) attack, Distributed Denial of Service (DDoS) bots, and fault analysis.

Different definitions of security:

Examining security of encryption, security of actual encryption algorithms, semantically secure systems, security of signatures.

Analysing provable security, explaining random oracles, security of encryption algorithms and encryption algorithms with random oracles.

Explaining provable security without random oracles, using examples such as strong RSA assumption, provable security-absolute assurance, signature and encryption schemes.

Analysing encryption techniques to include Key Encapsulation Mechanisms (KEMs), Data Encapsulation Mechanisms (DEMs), and hybrid public key encryption (PKE), for security.

LO3 **Demonstrate the use of cryptographic and cryptoanalysis tools for improving security in a virtual private network**

Cryptographic tools, methods and applications:

Secret Key to include secret key distribution, key exchange and signature schemes, Diffie-Hellman key exchange, digital signatures and authenticated key agreement.

Public Key to include one-way functions, obtaining authentic public keys, confidentiality and integrity, digital certificates and Public Key Infrastructure (PKI), analysing examples of PKI.

Hash functions to include designing hash functions, using hash functions in signature schemes, analysing hash functions.

Cryptographer role, responsibilities and continual professional development.

Cryptanalysis tools, methods and applications:

Attacking methods to include brute force, chosen plaintext, SQL injection, dictionary and rainbow tables.

Solving ciphers to include linear (i.e. Fast data Encipherment Algorithm); non-linear (i.e. linear masking), differential (i.e. mixed integer linear programming), block (i.e. simplified Tiny Encryption Algorithm).

Frustrating statistical cryptanalysis, including confusion and diffusion.

Impact of high-performance computing and quantum cryptography.

Web-based tools e.g. CrypTool, EverCrack, AlphaPeeler.

Cryptanalyst role, responsibilities and continual professional development.

Security case and system response:

Security case to include design of a system at network layer, crypto to meet defined security objectives, key management plan, evidence of system with required security controls, format e.g. Common Criteria Protection Protocol.

System response to include security objectives and common threats, assumptions, functional requirements and security controls e.g. technical, implementation, policy or process.

LO4 **Evaluate advanced encryption protocols and their application for an organisation considering a move to the cloud**

Assessing advanced encryption protocols and their applications:

Exploring access structures for secret sharing schemes for cloud security, general secret sharing, Reed-Solomon codes, Shamir sharing scheme.

Applying RSA key generation, securID and strategy in popular cloud environments.

Analysing Zero-Knowledge proofs, Sigma protocols, electronic voting systems.

Examining secure multi-party computation, the two-party case, multi-party cases including, honest-but-curious adversaries and malicious adversaries.

Evaluating different applications of cryptography and hybrid cryptosystems to include Cryptography as a Service (CaaS), digital cash, Bitcoin, Transport Layer Security (TLS) protocol, including configuration such as ciphersuites, blockchain, blockcloud and ZKsnarks.

Influencing factors affecting choice of cryptographic techniques for an organisation's move to the cloud:

Cost e.g. implementing encryption, network support, resourcing.

General considerations including suitability for business needs, infrastructure, scaling, reliability, support, storage capacity, content delivery, protection, user access and training.

Learning Outcomes and Assessment Criteria

Pass	Merit	Distinction
LO1 Analyse encryption ciphers and algorithms as methods to secure data in a cloud environment		
P1 Analyse the functions of stream cipher and block cipher, using a range of appropriate examples in practice. **P2** Produce code that implements mathematical ciphers and algorithms to encrypt and decrypt data.	**M1** Critically analyse the operational differences between stream cipher and block cipher, using a range of appropriate examples in practice.	**D1** Justify improvements introduced by stream ciphers compared to block ciphers for public and private key encryption.
LO2 Discuss security risks and issues related to public key encryption in practice		
P3 Discuss risks and issues in security of public key encryption schemes, using a range of appropriate examples in practice.	**M2** Analyse key benefits of encryption techniques including KEMs, DEMs and PKEs and the importance of securing public key systems.	**D2** Provide justified recommendations, synthesising different definitions of provable security, suitable for securing public key systems.
LO3 Demonstrate the use of cryptographic and cryptoanalysis tools for improving security in a virtual private network		
P4 Illustrate, using a diagram, encryption and decryption process functions in a PKI environment for a business scenario. **P5** Design a security case, representative of a business scenario, to solve a security threat.	**M3** Assess security risks and challenges of using cloud-hosted PKI in a private network. **M4** Implement the system designed, in response to a security case, using cryptographic and cryptanalysis methods or tools.	**D3** Provide a critical review of the implemented system in terms of how it meets defined security objectives and make suggestions for improvement.

Pass	Merit	Distinction
LO4 Evaluate advanced encryption protocols and their application for an organisation considering a move to the cloud		
P6 Evaluate the key benefits of using a range of cryptography and hybrid cryptosystems to improve cloud security. **P7** Assess common factors influencing an organisations choice of cloud solution(s) to improve security.	**M5** Critically analyse the use of selected cryptography and hybrid cryptosystems in protecting data within an organisation.	**D4** Justify the use of different cryptographic applications, for an organisation, that will inform their move to the cloud.

Recommended resources

Textbooks

BALACHANDRAN, M.J. (2020) *Cloud Engineering and Architecture Design Patterns.* Chennai: Notion Press.

CARLET, C. (2020) *Boolean Functions for Cryptography and Coding Theory.* Cambridge: Cambridge University Press.

CHAUBEY, N.K., PRAJAPATI, B.B. (2020) *Quantum Cryptography and the Future of Cyber Security.* USA: IGI Global.

GOYAL, D., BALAMURUGAN, S., PENG, S.L., VERMA, O.P. (2020) *Design and Analysis of Security Protocol for Communication.* USA: John Wiley & Sons.

MENEZES, A.J., VAN OORSHOT, P.C., VANSTONE, S.A. (2018) *Handbook of Applied Cryptography.* 2nd edn. Boca Raton: CRC Press, Taylor & Francis.

NIELSON, S.J., MONSON, C.K. (2019) *Practical Cryptography in Python: Learning Correct Cryptography by Example.* USA: Apress.

PACHGHARE, V.K. (2019). *Cryptography and Information Security.* 3rd edn. Delhi: PHI Learning.

SCHMEH, K. (2006) *Cryptography and Public Key Infrastructure on the Internet.* UK: Wiley.

STALLINGS, W. (2013) *Cryptography and Network Security: Principles and Practice*. UK: Pearson.

STINSON, D.R., PETERSON, M.B. (2018) *Cryptography: Theory and Practice.* 4th edn. Boca Raton: CRC Press, Taylor & Francis.

SWAMMY, S., THOMPSON, R., LOH, M. (2019) *Crypto Uncovered: The Evolution of Bitcoin and the Crypto Currency Marketplace.* (eBook) Palgrave Macmillan.

Journals

International Association for Cryptologic Research, Online

International Journal of Applied Cryptography, Online

International Journal of Network Security, Online

Journal of Emerging Trends in Computing and Information Sciences, Online

Web

ncsc.gov.uk — National Cyber Security Centre (General Reference)

Links

This unit links to the following related units:

Unit 5: Security

Unit 31: Forensics

Unit 32: Information Security Management.

Unit 31: Forensics

Unit code	**T/618/7444**
Unit level	**5**
Credit value	**15**

Introduction

This unit introduces students to digital forensics involving the use of specialised techniques to investigate the recovery, authentication and analysis of data on electronic data storage devices, as well as network security breaches and cyber attacks, using different tools and techniques.

With the current widespread use of digital devices, digital forensics has become an important part of the detection of crime by being able to identify details of what has been stored on digital devices in the past. Students will have the opportunity to learn about some of the lower-level structures of data storage devices and the techniques used to investigate them.

Among the topics included in this unit are: describing the process of carrying out digital forensics; forensic investigation legal guidelines and procedures; understanding low-level file structures of several operating systems (OS); creating a book disk to enable forensic examination of devices and undertaking a forensic examination of a device(s) and/or network security breaches and cyber attacks.

On successful completion of this unit, students will be able to carry out digital forensics in accordance with industry and legal guidelines and procedures using different tools. They will also understand the low-level file structures of several OS and be able to undertake digital forensic investigation of devices. As a result, they will develop skills such as communication literacy, critical thinking, analysis, reasoning and interpretation, which are crucial for gaining employment and developing academic competence.

Learning Outcomes

By the end of this unit students will be able to:

LO1 Examine the processes and procedures for carrying out digital forensic investigation

LO2 Discuss the legal and professional guidelines and procedures for carrying out digital forensic investigation

LO3 Use a tool or tools to conduct digital forensic investigation on devices or networks or cyber attacks

LO4 Develop a Test Plan and make some recommendations for use in digital forensic investigation.

Essential Content

LO1 Examine the processes and procedures for carrying out digital forensic investigation

The process of carrying out digital forensic investigation:

Discuss what is meant by digital forensics.

Identify the processes and procedures for carrying out digital forensic investigation, including policy and procedure development, evidence assessment, evidence acquisition, evidence examination (including extraction and analysis).

Sources of information:

Log files, digital system monitors, access control logs, file/folder access logs, operational anomalies, current and future threats, newly identified vulnerabilities, manufacturer's bulletins, hacker blogs and social media, collation of multiple sources to address and identify system security breach, root cause analysis.

LO2 Discuss the legal and professional guidelines and procedures for carrying out digital forensic investigation

Law enforcement:

Summarise APCO guidelines in relation to evidence collection, evidence preservation in a forensic investigation case. Discuss the activities of authorities, e.g. MI5/MI6, GCHQ and NSA, in relation to forensic investigations.

Legal and ethical considerations:

Discuss the following legal and ethical considerations when conducting a forensic investigation; Data Protection Act 2018; Computer Misuse Act 1990 and the Freedom of Information Act 2000.

Other stakeholders:

Forensic Science Society, BCS.

LO3 Use a tool or tools to conduct digital forensic investigation on devices or networks or cyber attacks

Tools required to conduct digital forensic investigation:

Hardware and software tools, e.g. Security Information and Event Management (SIEM) tools, system logs, penetration testing tools, network performance tools.

Conducting digital forensic investigation:

Conducting digital forensic investigation of devices, networks or cyber attacks to identify anomalies in observed digital system data structures, e.g. network packet data and digital system behaviours, including protocol behaviours, traffic levels and latency.

Identification and minimisation of false readings, e.g. negatives and positives generated by the available tools.

Examine Operating systems, e.g. MS-DOS, Windows, UNIX, Linux, MacOS, Android,.

LO4 Develop a Test Plan and make some recommendations for use in digital forensic investigation

Develop a Test Plan for digital devices or networks or cyber attacks:

Apply risk assessment and audit methodologies to identify potential vulnerabilities to inform a digital forensics Test Plan.

Recommendations for improving system security based on identified vulnerabilities and potential emerging threats.

Explore current 'best practice' recommendations from professional and legal bodies for conducting digital forensic investigations and developing Test Plans.

Learning Outcomes and Assessment Criteria

<table>
<tr><th>Pass</th><th>Merit</th><th>Distinction</th></tr>
<tr><td colspan="2">LO1 Examine the processes and procedures for carrying out digital forensic investigation</td><td rowspan="2">D1 Evaluate the advantages and disadvantages of conducting digital forensic investigation to improve system security.</td></tr>
<tr><td>P1 Discuss what is meant by digital forensics with the aid of diagrams/ pictures.
P2 Examine the processes and procedures for conducting digital Forensic investigation.</td><td>M1 Assess the importance of following a process or procedure when conducting digital forensic investigation.</td></tr>
<tr><td colspan="2">LO2 Discuss the legal and professional guidelines and procedures for carrying out digital forensic investigation</td><td rowspan="2">D2 Evaluate the impact of both following and not following guidelines in a legal case, with regard to digital forensic evidence.</td></tr>
<tr><td>P3 Examine law enforcement guidelines for conducting digital forensic investigations.
P4 Discuss legal and ethical requirements for conducting digital forensic investigations.</td><td>M2 Assess how ethical it is to conduct digital forensic investigation on a suspected individual, with reference to their legal rights.</td></tr>
</table>

Pass	Merit	Distinction
LO3 Use a tool or tools to conduct digital forensic investigation on devices or networks or cyber attacks		
P5 Determine hardware and software tools that can be used to conduct digital forensic investigation. **P6** Examine the file system structure of several operating systems	**M3** Compare two tools that can be used to conduct digital forensic investigation. **M4** Conduct a digital forensic investigation on a device or network or cyber attack.	**D3** Critically evaluate the forensic investigation carried out, suggesting improvements to the current digital forensic investigation guidelines, processes and procedures.
LO4 Develop a Test Plan and make some recommendations for use in digital forensic investigation		
P7 Develop a Test Plan for conducting a test on digital devices or networks or cyber attacks. **P8** Recommend security improvements based on test results.	**M5** Compare the recommendations for best practices for conducting digital forensics.	

Recommended Resources

Textbooks

Carrier. B. (2005) *File System Forensic Analysis*. Harlow: Addison-Wesley.

Farmer, D. and Venema, W. (2005) *Forensic Discovery*. Harlow: Addison-Wesley.

Hayes D. (2020) *A Practical Guide to Digital Forensics Investigations*. USA Pearson.

Jones, R. (2005) *Internet Forensics*. Sebastopol, O'Reilly.

Parasram, S. (2020) *Digital Forensics with Kali Linux.* 2nd edn. Packt Publishing

Sammes, A. and Jenkinson, B. (2007) *Forensic Computing: A Practitioner's Guide*. 2nd edn. London, Springer.

Web

bcs.org/membership/member-communities/cybercrime-forensics-specialist-group/	British Computer Society Forensics Specialist Group (General Reference)
gchq.gov.uk/	GCHQ (General Reference)
nsa.gov/	NSA (General Reference)

Links

This unit links to the following related units:

Unit 5: Security

Unit 30: Applied Cryptograpy in the Cloud

Unit 32: Information Security Management.

Unit 32: Information Security Management

Unit code	**J/618/7447**
Unit level	**5**
Credit value	**15**

Introduction

Organisations of all sizes need to protect their sensitive information from potential attackers, and simply having up-to-date firewalls, anti-virus and other infrastructure components is not enough to prevent breaches. All physical security devices, the teams who manage them, and the processes surrounding their management, need to be constantly monitored and evaluated to ensure that the organisation as a whole is protected. This is the concept behind an Information Security Management System (ISMS). An ongoing process to continually assess what the organisation deems its biggest threats, and what its most important assets are.

This unit introduces students to the basic principles of an ISMS and how businesses use them to manage the ongoing protection of sensitive information they hold effectively. There are many reasons for establishing an ISMS for an organisation, but one of the main goals is to enable the organisation to manage information security as a single entity, which can be monitored and continually improved on.

This unit covers information security management in a business context and will give students an understanding of how modern organisations manage the ongoing threats to their sensitive assets.

On successful completion of this unit, students will be able to describe what an ISMS is, how one is established, maintained and improved and describe the role that international standards play in developing an ISMS. Students will develop skills such as communication literacy, critical thinking, analysis, reasoning, and interpretation, which are crucial for gaining employment and developing academic competence.

Learning Outcomes

By the end of this unit students will be able to:

LO1 Explore the basic principles of information security management

LO2 Critically assess how an organisation can implement and maintain an Information Security Management System (ISMS)

LO3 Appraise an ISMS and describe any weaknesses it may contain

LO4 Examine the strengths and weaknesses of implementing ISMS standards.

Essential Content

LO1 Explore the basic principles of information security management

Principles of an ISMS:

What an ISMS is and why it is important to an organisation.

Policies, including privacy policy, acceptable use, information security, separation of duties and least privilege.

Internal and external risks, including impact, likelihood, quantitative, qualitative, vulnerabilities and threats.

Risk treatment, including avoid, transfer, accept or mitigate.

Managing compliance and stakeholders.

The role of a company's internal policies, including service level agreements (SLAs) with providers, impact on defining the scope and approach.

Use of recognised sources of threat intelligence and vulnerabilities to predict possible, current, and future threats, e.g. horizon scanning.

Key principles:

Understanding the key principles of an ISMS, including scope and boundaries, information classification, risk management methodology, risk treatment, statement of applicability, incident handling, physical security, controls that meet the organisation's business activity.

LO2 Critically assess how an organisation can implement and maintain an Information Security Management System (ISMS)

Implementing an ISMS:

Steps required to implement an ISMS, including creating a project mandate, initiation of the project, adopting a methodology for the ISMS, creating a management framework, identifying baseline security criteria, developing a risk management process, creating a risk treatment plan, measuring, monitoring and reviewing the results.

Planned design, including asset identification, stakeholder requirements, risk assessment, risk treatment planning, policy development, procedure development, senior management buy-in, audit (internal, external).

Maintaining an ISMS:

Elements and processes for maintaining an ISMS using a framework or an ISO standard, e.g. 27001, 27002.

Performance monitoring and continual improvement strategy.

LO3 **Appraise an ISMS and describe any weaknesses it may contain**

Appraising an ISMS:

Review ISMS documentation for potential weaknesses by examining audit and performance monitoring output, business impact analysis, review of current 'security culture' in the organisation.

Suggest improvements to an ISMS.

Planning an ISMS:

Business requirements, including strategic, functional and non-functional requirements of digital systems.

Impacts on the business, including interruption costs, cost of failure analyses, worst-case scenario, possibility of new impacts or vulnerabilities.

Audit and stages of audit for an ISMS:

Scoping and pre-audit survey, planning and preparation, fieldwork, analysis, reporting.

LO4 **Examine the strengths and weaknesses of implementing ISMS standards**

Implementing ISMS standards:

Determining ISMS scope, including leadership commitment, policy, organisational roles and responsibilities, actions to address risks, information security objectives.

Resources and competence, awareness, communications, documented information, operational planning, risk assessment, risk treatment, monitoring, measuring, analysis and evaluation.

Management review and taking nonconformity and corrective action, as well as continual improvement.

Key purpose of ISO standards:

ISO 27001:2013; the organisation and its context, expectations of interested parties.

Advantages and disadvantages of ISO 27001:2013 certification, annex A (ISO 27002:2013) controls, ISO 8000 and data standards.

Examination of principles and good practice recommended by computing professional bodies and their impact on organisational compliance.

Learning Outcomes and Assessment Criteria

<table>
<tr><th>Pass</th><th>Merit</th><th>Distinction</th></tr>
<tr><td colspan="2">LO1 Explore the basic principles of information security management</td><td rowspan="4">D1 Critically analyse what is required to establish and maintain an ISMS for a selected organisation, ensuring that the key principles are met.</td></tr>
<tr><td>P1 Examine the key principles of an ISMS and its relevance to the successful operation of an organisation.</td><td>M1 Analyse the benefits an effective ISMS can have on an organisation.</td></tr>
<tr><td colspan="2">LO2 Critically assess how an organisation can implement and maintain an Information Security Management System (ISMS)</td></tr>
<tr><td>P2 Assess the elements and processes required to establish and maintain an ISMS.</td><td>M2 Justify the steps required for implementing an ISMS for a selected organisation.</td></tr>
<tr><td colspan="2">LO3 Appraise an ISMS and describe any weaknesses it may contain</td><td rowspan="5">D2 Critically examine the advantages and disadvantages of the planned ISMS against the key ISO and international standards.</td></tr>
<tr><td>P3 Plan the design of an ISMS for a selected organisation, including an implementation map.
P4 Appraise the planned ISMS designed, against the organisational requirements.</td><td>M3 Justify the planned ISMS design for a selected organisation by following the stages of audit.</td></tr>
<tr><td colspan="2">LO4 Examine the strengths and weaknesses of implementing ISMS standards</td></tr>
<tr><td>P5 Recognise the purpose of the key ISO and international ISMS standards.</td><td>M4 Analyse the relationship between ISO standards and establishing an effective ISMS in an organisation.</td></tr>
</table>

Recommended Resources

Textbooks

Alexander, D., Finch, A., Sutton, D. and Taylor, A. (2020) *Information Security Management Principles* BCS. 3rd edn. BCS The Chartered Institute for IT.

Calder, A. and Watkins, S. (2019*) IT Governance: An International Guide to Data Security and ISO27001/ISO27002*. 7th edn. Kogan Page.

Journal

Information Management & Computer Security - Emerald Insight

Web

www.iso.org	International Organisation for Standardization – ISO/IEC 27001 – Information Security Management (General Reference)

Links

This unit links to the following related units:

Unit 5: Security

Unit 30: Applied Cryptography in the Cloud

Unit 31: Forensics.

Unit 26: Big Data Analytics and Visualisation

Unit code	**F/618/5664**
Unit level	**5**
Credit value	**15**

Introduction

Raw data can be complicated, confusing and a challenge to understand. But when raw data is organised and structured properly it can reveal patterns and information that can be very powerful in business decision making. Without the ability to organise and visualise data, key information would otherwise remain hidden in raw data. Once a business can understand historic patterns of data sets this information can help predict future trends and behaviours.

Data and visualisation is an area which has seen rapid advancement and there has been considerable challenges for data specialists to develop the skills, experience and growth required to maintain innovation in the sector. As data continues to be the fuel for the digital economy, this area remains a constant topic of conversation for organisations, governments and the public who share an interest in its growing commercial use, manipulation, and presentation.

This unit introduces students to the concepts of big data and visualisation and how this is used for decision making. It explores the industry software solutions available to investigate and present data, before assessing the role and responsibility of data specialists in this current environment. Topics including data driven decision-making, manipulating data and automation, and building ethics into a data-driven culture are examined. Students will demonstrate their use of tools and software to manipulate and prepare a visual presentation for a given data set. They will also assess how data specialists are responsible for adhering to legislation and ensuring data compliance.

On successful completion of this unit students will be able to investigate the value of data for decision making to both end users and organisations, compare how different industry leading tools and software solutions are used to analyse and visualise data, carry-out queries to summarise and group a given data set and analyse the challenges faced when building ethics into a data-driven culture. Students will have the opportunity to progress to a range of roles within the digital sector, and will develop industry-led skills, analysis, and interpretation, which are crucial for developing practical experiences with big data and gaining employment.

Learning Outcomes

By the end of this unit, students will be able to:

LO1 Examine data visualisation for decision making of complex data sets

LO2 Discuss statistical and graphical tools and techniques used to present big data for a given use case

LO3 Demonstrate statistical and graphical techniques used to present big data as a visualisation

LO4 Investigate the challenges faced by data professionals in carrying out their role.

Essential Content

LO1 **Examine data visualisation for decision making of complex data sets**

Big Data:

Explore common fundamental concepts e.g. Bayesian classification, rule-based classification, The 'Vs' of big data (Volume, Velocity, Variety, Variability, Veracity, Visualization, and Value).

Big data lifecycle to include purpose, capturing data, searching and filtering, retrieving data for processing, combining multiple data sources, validation and cleansing, visualisation, analysis and querying, utilisation and storage, obsolete and deleted data.

Visualisation:

Identify the target audience needs, e.g. context, reporting, dissemination, accessibility, breadth of data, depth of analysis.

Explain the phases of data visualisation design process to include formulating the brief, working with data, establishing editorial thinking and developing design solution.

Apply principles of good design to data visualisation e.g. Dieter Rams' Ten Principles for Good Design, Gestalt principles of visual perception and Pareto Chart.

Evaluate effective visual elements e.g. charts, graphs, plots, tables, points, lines, bars, area, maps, narratives, metaphors, symbols and aesthetics e.g. position, size, shape, colour and transparency.

Data for decision making:

Explore processes of data driven decision making (DDDM) e.g. define objective, establish hypothesis, identify data need, build data process, sampling methods, collect data, analyse data, interpret results and make decision.

The role of the Data Analysis Lifecycle as part of DDDM (e.g. Discovery, Data preparation, Model Planning, Model Building, Operationalise, Communicate results).

Discuss the advantages of data driven decision-making e.g. continuous improvement and planning, collaborative decisions, reduce costs, real-time insights and new opportunities, digital literacy and data-driven cultures.

Challenges e.g. inconsistent and unstandardised data, aligning decision making with business strategy, bias and discrimination, descriptive vs. predictive trends and probabilities.

LO2 **Discuss statistical and graphical tools and techniques used to present big data for a given use case**

Statistical and graphical techniques for big data analysis and visualisation:

Analyse and apply big data analytics techniques taking account of different data structures and database designs e.g. descriptive, prescriptive, diagnostic and predictive analytics.

Apply principles of mathematics and statistics for analysing data sets.

Explore the various kinds of analysis techniques e.g. anomaly detection, cluster, association by rule, classification and regression analysis.

Examine how to organise semi-structured and unstructured data variety e.g. word-cloud visuals, data catalogue, taxonomies and ontologies.

Forecasting estimates of future values e.g. applied forecasting and decision tree algorithms.

Industry leading tools and software solutions to analyse data:

Apply tools to analyse data e.g. programming or scripting languages such as Python or R and associated libraries, Application Programming Interfaces (APIs).

Industry leading tools and software solutions to visualise data:

Apply leading tools to a solution e.g. Microsoft Excel, Tableau, PowerBI and Azure, AWS, Oracle Visual Analyzer, Qlikview, Canvas, SAS Visual Analytics.

Explore how user experience and domain context influences approaches to data analytics and visualisation.

LO3 **Demonstrate statistical and graphical techniques used to present big data as a visualisation**

Manipulating data:

Construct activities using industry software to manipulate data e.g. importing datasets, data cleansing, data frame manipulation, testing and training a model, summarising analysis process and steps taken.

Apply query basics e.g. reports, calculate aggregate statistics, use built-in functions summarising and grouping data.

Explore advanced data manipulation and automation concepts e.g. generalised linear models and regression, multilevel modelling and techniques, data pipelines, machine learning and deep reinforcement learning (DRL).

Prepare visual presentations:

Visual presentations to include using insight analysis to understand data in context, selecting visual elements and aesthetic design e.g. find and filter content in dashboards, view and export data from dashboards to create report, presentation or infographic.

Data set requirements:

Understanding the data and its context including summary of data collection, sampling procedures and data type; stakeholder requirements, interests and needs.

LO4 **Investigate the challenges faced by data professionals in carrying out their role**

Roles and responsibilities:

Explain roles in a data-driven industry e.g. data analyst, data scientist, data engineer, visualisation specialist, data administrator, business analyst, middle-managers and senior management teams.

Explore the responsibilities of a data specialist e.g. preparing, analysing, modelling, managing and visualising data, and storage and access rights.

Strategies to ensure data compliance:

Explain organisational data architecture, policies, standards and rules e.g. how data is stored, managed, used and disseminated.

Assess data protection, informed consent and privacy issues for compliance e.g. personally identifiable information, protected health information, General Data Protection Regulation (GDPR) rights obligations, enforcement and regulatory legal penalties.

Explore and select the most appropriate industry compliance management software tools e.g. Microsoft Compliance Manager, AWS Compliance, IBM DataOps.

Identify and escalate quality risks in data analysis with suggested mitigation or resolutions as appropriate.

Challenges for data specialists:

Understand challenges such as applying data governance framework to ensure value of outcomes, accountability, trust, collaboration, transparency, risks and security, and role of the data steward.

Explain how to guard from poor practice e.g. cherry picking, disclosure of assumptions, conflict of interest, bias from single view and/or choice of technique.

Risks and challenges to combing data from different sources in data analysis activity.

Develop ethics into a data-driven culture and joining community of good practice e.g. Data for Good Exchange (D4GX); Fairness, Accountability and Transparency in Machine Learning group (FAT/ML), Data Ethics Framework (gov.uk).

Learning Outcomes and Assessment Criteria

Pass	Merit	Distinction
LO1 Examine data visualisation for decision making of complex data sets		
P1 Explain the fundamental concepts of big data and its value in decision making for end users and organisations. **P2** Examine the processes of data driven decision making (DDDM) when using complex data sets.	**M1** Discuss the advantages and challenges to an organisation of using complex data sets for decision making.	**D1** Predict the potential impact of using complex data sets on both users and organisations for decision making.
LO2 Discuss statistical and graphical tools and techniques used to present big data for a given use case		
P3 Discuss statistical and graphical tools and techniques used in industry for big data manipulation and visualisation.	**M2** Assess the suitability of industry leading tools and software solutions for analysing and visualising data for the given use case.	**D2** Evaluate how well the chosen data preparation and manipulation methods, the tools selected, and the data derived will impact on business decision making for the given use case.
LO3 Demonstrate statistical and graphical techniques used to present big data as a visualisation.		
P4 Demonstrate the use of data manipulation and automation to present a visualisation for a given user case.	**M3** Interpret the findings derived from the data manipulation to support conclusions made.	
LO4 Investigate the challenges faced by data professionals in carrying out their role.		
P5 Investigate the different roles, responsibilities and key issues faced by data specialists in their day-to-day role.	**M4** Review the different strategies used by data specialists to ensure data compliance.	**D3** Evaluate the impact of the key issues faced by data specialists when working in a data-driven culture.

Recommended resources

Textbooks

DIETEL, P. (2020) *Intro to Python for Computer Science and Data Science: Learning to Program with AI, Big Data and The Cloud*. London: Pearson.

FRANKS, B. (2020) *97 Things About Ethics Everyone in Data Science Should Know*. USA: O'Reilly Media.

GRAESSER, L. and KENG, W.L. (2020) *Foundations of Deep Reinforcement Learning: Theory and Practice in Python*. London: Addison-Wesley Professional.

KIRK, A. (2019) *Data Visualisation: A Handbook for Data Driven Design*. London: Sage Publications.

KNAFLIC, C. N. (2015) *Storytelling with Data: A Data Visualization Guide for Business Professionals*. USA: John Wiley & Sons.

LOUKIDES, M., MASON, H. and PATIL, D.J. (2018) *Ethics and Data Science*. USA: O'Reilly Media.

MARR, B. (2017) *Data Strategy: How to Profit from a World of Big Data, Analytics and the Internet of Things*. London: Kogan Page.

McCORMICK, K., and SALCEDO, J. (2017) *SPSS Statistics for Data Analysis and Visualization*. USA: John Wiley & Sons.

ROSS, J. (2019) *Data Science Foundations Tools and Techniques: Core Skills for Quantitative Analysis with R and Git.* London: Addison-Wesley Professional.

VIESCAS, J.L. (2018) *SQL Queries for Mere Mortals: A Hands-On Guide to Data Manipulation in SQL.* 4th edn. London: Addison-Wesley Professional.

WILKE, C.O. (2019) *Fundamentals of Data Visualization: A Primer on Making Informative and Compelling Figures.* USA: O'Reilly Media.

Journals

Big Data & Society, Online

Journal of Data Science, Statistics and Visualisation, Online

Journal of Big Data, Online

International Journal of Computer Applications, Online

Web

ukdataservice.ac.uk	UK Data Service (General Reference)
gov.uk	UK Government (Data Ethics Framework)

Links

This unit links to the following related units:

Unit 4: Database Design and Development

Unit 8: Data Analytics

Unit 24: Advanced Programming for Data Analysis

Unit 33: Applied Analytical Models.