Validation Report

BN120

Bachelor of Science (Honours) in Information Security and Digital Forensics

(240 ECTS credits leading to NFQ Level 8 Award)

BN034

Bachelor of Science in Information Security and Digital Forensics

(180 ECTS credits leading to NFQ Level 7 Award)

BN311

Bachelor of Science in Information Security and Digital Forensics

(Add on award to BN002 - 60 ECTS credits leading to NFQ Level 7 Award)

BN420

Bachelor of Science (Honours) in Information Security and Digital Forensics

(Add on award to BN034 - 60 ECTS credits leading to NFQ Level 8 Award)

Introduction

The Institute of Technology Blanchardstown was established in 1999. The mission of the Institute is to serve its students and the community by meeting the skills needs in the economy and increasing the level of participation in third-level education and training, particularly in Dublin North-West and its environs.

The Institute in 2006 was awarded delegated authority enabling the development, validation, implementation and continuous improvement of taught higher education and training programmes up to and including level 9 of the National Framework of Qualifications.

In keeping with the Institute's mission statement, course and programme development is on-going. Information security and digital forensics was identified as a potential area for development and further investigation indicated a strong demand for courses in this academic area. This programme supports the mission of the Institute and facilitates much wider access to the Institute by a cohort of potential students whose needs are currently not being met.

The purpose of this document is to report on the findings of the peer review panel established to validate this proposed programme against the criteria for the validation of programmes as stipulated in the Institute policy document 2MP01[I].

This submission by the School of Informatics and Engineering evolved through:

- examining the competence, expertise and experience of it's staff in addition to the strategy of the department/school/Institute and Government educational policy

- research evidence indicating an industry demand for appropriately qualified graduates with a specialised skill set within the area of information security and digital forensics.

[I] 2MP01 Design, validation and accreditation of new academic programmes

Programme overview

The proposed programme is a 4 year honours degree programme with embedded awards at Higher Certificate (level 6, NFQ[I]) and Ordinary Degree (level 7, NFQ). Modules offered in the first four semesters of this programme will be common with the Higher Certificate in Science in Computing in Information Technology (BN002) currently delivered by the School of Informatics and Engineering.

This programme is designed to give students a comprehensive understanding with specific abilities and associated best practices in the areas of computing with specialisation in information security and digital forensics. The knowledge and skills a graduate of this programme will develop have been categorised within the following thematic areas of expertise:

- Software engineering
- Infrastructure and forensics
- Networking and security
- Web based technologies
- Data abstraction
- Professional development

The software engineering theme will provide the student with an essential skill set as all applications are written in programming languages, thus knowledge of this area is essential to understanding vulnerabilities in applications and control systems.

The infrastructure and forensics theme will provide students with hands on experience of disassembling and re-assembling a computer, learning about micro-chips and how the processor and memory work. Critical to their knowledge will be how data is stored and the workings of the operating system. Forensics investigations will allow the student to explore the steps involved in acquiring, examining, analyzing and the presentation of digital evidence stored in computers, external hard drives, memory sticks and network storage devices in the form of documents, images, emails, user profiles and log files.

The networking and security theme involves the building and configuration of both local and wide area networks teaching the student how to protect networks, enabling secure communications over robust systems.

[I] National Framework of Qualifications

Web based technologies are at the core of internet development thus a solid foundation in web and multimedia technologies is essential to student competencies in the proposed programme.

The data abstraction theme will allow the student to develop skills in modelling real-world situations of interest and learn how to analyse data and present the results. Core data structures and modelling techniques will be taught together with essential mathematical knowledge.

The professional development theme introduces the student to modules specifically concerning their professional practice, personal development, lifecycle development, project management and working in the information security and digital forensics industry. The students' working practices will continually evolve through the completion of project work at all levels of the programme, forming core taught elements of these modules.

Initially students will develop a strong set of technical skills covering the essential areas of computing, programming, networking, computer systems, web development and mathematics. This foundation of knowledge and skills will be then built upon by introducing the student to the disciplines of forensics investigation, digital forensic analysis, network security, secure communications, cyber crime investigations, biometrics, data mining, risk management, business continuity and disaster recovery. Under pinning the student development are the group and individual project modules selected from information security and digital forensics real–world situations. The final year of the course will consolidate and integrate skills and knowledge so as to make the graduates of this Bachelor of Science (Honours) programme at ITB of immediate value to industry.

Programme detail

Programme title Bachelor of Science (Honours) in Information Security and Digital Forensics

Award title Bachelor of Science (Honours)

NFQ level 8

ECTS[I] credits 240

Programme code BN120

Banner code BN_KISDF_8

Embedded award

Banner code	ITB code	Programme title	Award title	ECTS credits	Format
BN_KISDF_7	BN034	Bachelor of Science in Information Security and Digital Forensics	Bachelor of Science	Level 7 180 credits	Ab initio

Add on awards

BN_ KISDF_D	BN311	Bachelor of Science in Information Security and Digital Forensics	Bachelor of Science	Level 7 60 credits	Add on to BN002
BN_ KISDF_B	BN420	Bachelor of Science (Honours) in Information Security and Digital Forensics	Bachelor of Science (Honours)	Level 8 60 credits	Add on to BN034

[I] European Credit Transfer and Accumulation System

Panel members

Chairperson	Mr. Stephen McManus Dundalk Institute of Technology
Panel member 1	Dr. Pavel Gladyshev University College Dublin
Panel member 2	Dr. Vivienne Mee Deloitte and Touch
Panel member 3	Mr. William Farrelly Letterkenny Institute of Technology
Panel member 4	Dr. Mícheál ÓhÉigeartaigh Waterford Institute of Technology
In attendance	Dr. Diarmuid O'Callaghan IT Blanchardstown Mr. Michael Keane IT Blanchardstown
Date of Panel Meeting	Thursday 21st May 2009

Institute staff present

Session I Meeting with President, Head of School, Head of Department & Programme Leader

Dr. Mary Meaney, President

Mr. Larry McNutt, Head of School of Informatics and Engineering

Dr. Brian Nolan, Head of Department of Informatics

Dr. Anthony Keane, Department of Informatics

Session II Meeting with Lecturing Staff

Mr. Larry McNutt	Dr. Brian Nolan
Dr. Anthony Keane	Mr. Tom Nolan
Ms. Geraldine Gray	Mr. Hugh McCabe
Mr. Michael O'Donnell	Ms. Orla McMahon
Mr. Cormac McMahon	Mr. Ivan Smyth
Mr. Barry Kirkpatrick	Ms. Laura Keyes
Mr. Mark Cummins	Mr. Damian Cox
Mr. Conn Cremin	Ms. Aoife Fox

Panel findings

In evaluating the appropriateness, quality and proposed operation of this programme the following criteria have been considered and are hereby reported upon:

Strategic planning

The panel was satisfied that the programme is in keeping with the Institute's mission, that it does not constitute redundant provision and that it makes efficient use of resources.

Evidence of consultation

The panel heard how a comprehensive research effort was undertaken to validate the need for and the preferred structure and characteristics of the proposed programme.

Drafts of the proposed curriculum were considered by independent industry experts. A list of module areas and external reviewers is shown below:

Module area	External reviewer
Information security	ISSA[I] members, Hewlett-Packard, Symantec, ELAN, Cernam Ltd, BH Consulting
Digital forensics	Deloitte, Rits, Espion

The panel also heard how extensive secondary research activity explored industry publications, Irish Government and European Union publications, trade journals, print media articles, web resources and the output of the last programmatic review within ITB.

The panel was satisfied with this consultation.

[I] Information Systems Security Association

Learner employment potential

It is envisaged that graduates of the Bachelor of Science (Honours) in Information Security and Digital Forensics will have the knowledge and skills to take up employment in a broad number of areas within the information security industry, including

- Technical experts in digital forensics
- Forensics investigators
- IT security consultants
- Project managers
- IT system and compliance auditors
- Research and development contributors

Graduates of this level 8 programme will be imbued with the critical thinking and reflective abilities typical of a leadership role in the information security industry. They will be able to draw upon a high level of technical knowledge and design, creative and critical thinking to drive their working teams to reassess and reconfigure existing material and new content to produce work of genuine technical merit.

The philosophy of the programme is to stress the theoretical and technical fundamentals irrespective of the latest developments in hardware and software. Therefore, its graduates will be able to operate as effective digital forensics practitioners by applying many different tools and technologies and will be in a position to drive their own professional development by learning new digital forensics production techniques as they arise and assess their place in the broad spectrum of available technology.

It is envisaged that graduates of the level 7 programme will occupy an appropriate leading practitioner role in a relevant organisation. They will be able to apply the broad range of technical skills they have acquired to a variety of projects in the areas of work described above, complemented by the technical and project design skills to generate new ideas and operate in an interdisciplinary environment. They will be able to operate as effective digital forensics practitioners by applying many different tools and technologies and will be in a position to learn new tools and techniques as they arise, as directed in the workplace.

Protection of learners

Section 43 of the Act[I] does not apply.

Quality assurance

The panel was informed of how the proposed programme had been developed and approved internally whilst complying with the Institute's quality assurance policies and procedures. The panel concurred that said policies and procedures had been applied to the development of the proposed programme.

Programme titles and award titles

Following discussion, the panel was satisfied that the title of the proposed programme, and its embedded sub-award is clear, accurate and fit for the purpose of informing prospective learners and other stakeholders of the focus of the programme. However, the panel recommended that the words "in Computing" be inserted into the programme title. See panel recommendations.

Ethics

The panel was satisfied that the Institute has internal policies and procedures in place to ensure that all teaching, learning or research activity across the spectrum of NFQ levels is conducted / delivered in a manner that is both morally and professionally ethical.

Unity

The panel found that the programme design is consistent with HETAC's[II] policy on accumulation of credits and certification of subjects, that it has an underlying unifying theme with modules bonded by linkages being either implicit or explicit. It was also clear to the panel how the standards of knowledge, skill and competence evolve throughout the programme as a whole.

[I] Qualifications (Education and Training) Act, 1999
[II] Higher Education and Training Awards Council

Teaching and learning

The panel discussed with staff of the Institute the various modes of interaction with learners. Evidence of a clear dialogue was confirmed, enabling learners to develop and have available to them the support of academic staff.

Course management arrangements were discussed and deemed adequate, these included:

- survey of students by lecturer
- summary of survey of students by lecturer
- survey of students by department
- course boards

The panel was satisfied that the necessary staffing levels exist to deliver the programme and were suitably impressed with the qualifications, experience, and competence of the Institute's staff. The panel commented on the obvious enthusiasm of staff involved in the development of the programme.

Relevance

In today's society, business practices rely on digital information more now than at any time in the past for availability, integrity and confidentially. Underlying these requirements are hardware, software and communication systems, the basic components of the digital information infrastructure, each with its own specific set of vulnerabilities that can affect the performance and integrity of technological information systems.

This reliance on vulnerable information systems has been exploited by both mischief makers and criminal organisations and their activities are widely reported in the media, almost daily. With the widespread adoption of wireless networks, an increase in hacking activity has been observed with people attempting to gain access to an organisation's information system over the internet by exploiting vulnerabilities in the applications and security implementation used to protect the data.

The risk to business data has been recognised by the following:

- The Industry Security sector has seen a large increase in the number of industrial recognised certification programs dealing with Information

Security such as CISSP[I], ECH-Ethical Hacker[II], SANS institute[III], CompTIA, Cisco, etc.

- Governments have created special legislation dealing with computer crime in its own right and see computer and digital forensics playing a greater role in getting evidence for successful prosecutions.

- Organisations such as Microsoft have established special boards to deal with security such as the Trustworthy Computing Academic Advisory Board. Other organisations make it their business to work in security such as Symantec, McAfee and F-Secure.

The need for more specialised network security and computer forensics education and research has been outlined in many survey reports as follows:

- According to the results of "The ISSA/UCD Irish Cybercrime Survey 2006: The Impact of Cybercrime on Irish Organisations" report, Irish organisations are significantly affected by cybercrime where virtually all (98%) of respondents indicated that they had experienced some form of cybercrime with losses of productivity and data being the main consequences. The ISSA/UCD Irish Cybercrime Survey for 2008 focused on cybercrime incidents occurring in 2007.

- The annual Ernst & Young Global Information Security Survey 2008 has revealed that global respondents ranked privacy and data protection among the top three drivers of information security. Also reported is that despite tightening economies, the survey indicates that organizations are increasing investments in information security and more organizations are adopting international security standards.

Learner assessment

Through discussion with the design team, and from the submission document itself it was explained in detail to the panel the multiple modes of assessment, both formal and informal that will be employed on the programme. These included a combination of in-class tests, formal examinations, assignments, reports, projects, presentations and seminars. The panel also heard how coursework assessments where appropriate, will include individual and teamwork assignments, projects, class and laboratory exercises, workshop practice, and assignments. The panel however raised concerns over the volume of written exam assessment for the proposed programme and encouraged a more innovative approach where assessment is concerned. See recommendations.

[I] Certified Information Systems Security Professional
[II] EC Council Ethical Hacking Certification
[III] SysAdmin Audit Network Security Institute

Standards of knowledge, skill and competence

The panel felt having reviewed the syllabi and assessment methods for the programme that learners would be capable of attaining the standards of knowledge, skill or competence relevant for this award.

Access, transfer and progression

The programme incorporates the established procedures for access, transfer and progression allowing students to choose from various entry and exit points that support clear transfer and progression routes within the National Framework of Qualifications (NFQ).

Decision of the panel

The panel recommends the validation of the proposed programme, its embedded award and add on awards namely:

Banner code	ITB code	Programme title	Award title	ECTS credits	Format
BN_KISDF_8	BN120	Bachelor of Science (Honours) in Information Security and Digital Forensics	Bachelor of Science (Honours)	Level 8 240 credits	Ab initio
BN_KISDF_7	BN034	Bachelor of Science in Information Security and Digital Forensics	Bachelor of Science	Level 7 180 credits	Ab initio
BN_ KISDF_D	BN311	Bachelor of Science in Information Security and Digital Forensics	Bachelor of Science	Level 7 60 credits	Add on to BN002
BN_ KISDF_B	BN420	Bachelor of Science (Honours) in Information Security and Digital Forensics	Bachelor of Science (Honours)	Level 8 60 credits	Add on to BN034

Panel observations

The panel congratulated the programme design team complimenting them on the quality and detail of the programme as proposed in the submission document. They concurred on the wide range of skills a graduate of this programme seeking employment would require. The panel felt that the development of these skills was well reflected in what they deemed to be a well blended, balanced and above all a relevant, responsive programme addressing the identified needs of industry, both local and national.

Panel recommendations

1. Clearly articulate and make explicit within all published material and make advertising arrangements as necessary to alert students to the fact that the first two years of this programme are common to another previously validated programme, BN002 Higher Certificate in Science in Computing in Information Technology, and specialisation occurs in years 3 and 4.
2. Consider amending the programme title to "Bachelor of Science (Honours) in Computing in Information Security and Digital Forensics".
3. Consider including a module on "Irish and EU Law" incorporating ethical considerations with regard to data protection, possibly in year 3.
4. Reconsider the credit weighting of critical final year modules.
5. Revisit the learning modes to reflect the actual delivery of modules while also considering the delivery of at least one module fully online.
6. Reconsider the volume of written exam assessment and be more innovative in the mode of assessments used to ensure that the learning outcomes are adequately assessed overall.
7. Review the content and terminology of the learning outcomes to ensure consistency, equity and relevance to specific NFQ levels for the programme and individual modules.
8. Reconsider class contact hours with a view to including a greater degree of self directed learning in the final year of the programme.
9. Make other technical and minor amendments as discussed at the panel meeting including:
    - Entry requirements
    - Standardised modular content in syllabus submission
    - Pre requisites

Panel signatures

Chairperson

Mr. Stephen McManus _____ Date _____

Secretary

Dr. Diarmuid O'Callaghan _____ Date _____