

# Programme Review



## **Bachelor of Science (Honours) in Computing in Information Security and Digital Forensics BN120**

**Department of Informatics**

**Peer-review panel report**

7<sup>th</sup> June 2013

## **Table of contents**

Executive summary.....	1
Preamble .....	1
Programmes reviewed.....	2
Peer-review panel.....	3
Consultation .....	4
Documentation submitted for consideration .....	5
Panel meeting.....	6
Decision of the panel .....	10
Panel observations .....	11

## 1. Executive summary

- 1.1. The Department of Informatics, Institute of Technology Blanchardstown undertook a review of the structure and content of years three and four of its information security and digital forensics suite of programmes. Resulting from this review a submission document was produced outlining proposed changes to the content and structure of the programmes. An external peer-review expert panel was established by the Registrar. This panel met on the 5<sup>th</sup> June 2013 to consider the submission document and to meet with academic staff responsible for the management and delivery of the programmes. This report identifies the findings of this peer-review expert panel.
- 1.2. The overall recommendation of the panel was that all proposed changes to the programme structure, existing syllabi and proposed new syllabi made in the submission document be accepted. The panel recommended that the suite of information security and digital forensics programmes be accredited until the next programmatic review. Some specific conditions and recommendations have been made in the light of continuous improvement in this report to qualify the scope of this overall recommendation.
- 1.3. The panel was impressed with the proposed new offering and of the opinion that it would produce graduates of immediate value to the digital forensics and cyber security sector. The panel commended the staff of the Department on the depth of consultation undertaken in the programme redesign and the level of open and frank dialogue throughout the various engagements during the visit.

## 2. Preamble

- 2.1. The Bachelor of Science (Honours) in Computing in Information Security and Digital Forensics programme was originally validated in 2009. In 2010 the School of Informatics and Engineering, Institute of Technology Blanchardstown undertook a review of its programmes as per Institute policy relating to institutional review and particularly the monitoring and evaluation of academic programmes. Because the programme had only been validated the previous year it was not reviewed at that time. Experience gained in delivering this programme to date from the perspective of lecturers, students and industry with whom we are engaged, pointed to areas for improvement in the programme.
- 2.2. The peer-review group produced a report of their findings (this document) and this will be reported to the Academic Council of the Institute as per agreed quality assurance policy and procedures.

### 3. Programmes under review

Banner code	ITB code	Programme title	Award title	NFQ level / ECTS credits	Format
BN_KISDF_8	BN120	Bachelor of Science (Honours) in Computing in Information Security and Digital Forensics	Bachelor of Science (Honours)	NFQ level 8 240 credits	Ab initio

#### Embedded awards

BN_HSACD_7	BN034	Bachelor of Science in Computing in Information Security and Digital Forensics	Bachelor of Science	NFQ level 7 180 credits	Ab initio
BN_KISDF_D	BN311	Bachelor of Science in Computing in Information Security and Digital Forensics	Bachelor of Science	NFQ level 7 60 credits	Add on to BN002
BN_KISDF_B	BN420	Bachelor of Science (Honours) in Computing in Information Security and Digital Forensics	Bachelor of Science (Honours)	NFQ level 8 60 credits	Add on to BN034

The schedule and syllabus of years one and two, the NFQ level 6 component, of our computing programmes are common and were not reviewed at this time.

**Peer-review panel**

Dr. Stephen Cassidy	Dean of Academic Quality Enhancement Cork Institute of Technology
Ms. Janice O'Connell	Head of Department of Computing Limerick Institute of Technology
Dr. Vivienne Mee	Rits Computer Forensics Ltd
Mr. William Farrelly	Letterkenny Institute of Technology
Mr. William Bailey	IBM

Dr. Stephen Cassidy kindly agreed to chair this panel.

Also in attendance:

Dr. Diarmuid O'Callaghan	Registrar Institute of Technology Blanchardstown
Mr. Michael Keane	Quality Assurance Officer Institute of Technology Blanchardstown

Date of panel visit:

Wednesday 5<sup>th</sup> June 2013

## 4. Consultation

### 4.1. Management consulted during panel meeting:

Dr. Larry McNutt	Head of School of Informatics and Engineering
Dr. Brian Nolan	Head of Department of Informatics

### 4.2. Academic staff consulted during panel meeting:

Dr. Anthony Keane	Dr. Markus Hofmann	Mr. Tom Nolan
Mr. Mark Cummins	Ms. Laura Keyes	Mr. Arnold Hensman
Ms. Irene Murtagh	Mr. Mark Lane	

### 4.3. Students:

All current cohorts of information security and digital forensics students, including recent graduates, were consulted in preparing the submission document.

### 4.4. Industry:

Over the last two years academic staff responsible for the management and delivery of this programme have been active with industry practitioners through various organisations including OWASP<sup>1</sup>, IRISS<sup>2</sup> and Information security Ireland (ISI). Relationships have been established with companies such as IBM, Rits, Espion, An Post, Eircom, Amazon, Facebook, Google and many more. Feedback from these and the careful monitoring of job advertisements have contributed to the re-design of this programme.

<sup>1</sup> The Open Web Application Security Project (OWASP) is an open-source application security project including corporations, educational organisations, and individuals from around the world.

<sup>2</sup> Irish Reporting and Information Security Service

## **5. Documentation submitted for consideration**

5.1.1. The submission document outlined the following:

- Rationale for programme review
- Consultation
- Employment and career opportunities for graduates
- Progression opportunities for graduates
- Resource implications
- Current programme content and structure
- Proposed revised content and structure – all new modules not previously validated
- Curricula vitae of relevant academic staff within the Department of Informatics
- Relevant Institute policies and procedures

## **6. Private panel meeting:**

- 6.1. It was noted that the programmatic review process is part of a suite of quality assurance processes agreed with QQI (Quality and Qualifications Ireland, formerly HETAC) and in accordance with the provisions of Section 28 of the Qualifications (Education and Training) Act 1999. This process involves self-evaluation with recommendations of amendments to the existing approved course schedule with associated justification.
- 6.2. As per agreed procedure, the Registrar acted as secretary to the group.
- 6.3. It was noted that the Academic Council has responsibility for ensuring that recommendations of this panel report are implemented.
- 6.4. The Chair presented the context of the panel review and noted that the purpose of programmatic review is to:
  - Facilitate a reflective self-evaluation within the relevant Department to allow a critical evaluation of a programme and its constituent embedded awards with consideration of this self-evaluation by a panel of peers drawn from education and industry;
  - Facilitate a review of all matters pertaining to the management and delivery of a programme indicating how they have been updated in light of changing environmental conditions and recent knowledge.
- 6.5. The roles and responsibilities of the panel as listed in Institute policy document 2MP17 “Roles and responsibilities of external experts on validation and review panels” were noted.

## **7. Meeting with Head of School, Head of Department and Programme Leaders:**

- 7.1. The Head of Department of Informatics outlined to the panel the rationale for the proposed revised content and structure of the programme giving a brief overview of the consultation undertaken.
- 7.2. Two clear aims of the proposed revised programme were identified by the programme leaders namely:
  - 7.2.1. Revise the programme and award title to ‘Bachelor of Science (Honours) in Computing in Digital Forensics and Cyber Security’.
  - 7.2.2. Rationalise and consolidate the number and volume of modules both mandatory and elective.
- 7.3. Programme title

A lengthy discussion followed with regard to the proposed title change within which the panel sought further clarification that the title as proposed was fit for purpose for informing prospective learners and employers of the skill sets a graduate would acquire on successful completion of the level 7 and level 8 awards. The panel noted that although the constituent modules content as proposed reflected the new

title the module titles themselves were too generic. This was discussed in greater detail during the meeting with academic staff delivering the programme.

#### 7.4. Revised structure

The rationale for the proposed revised structure was explored. The programme design team cited several operational issues, structural weaknesses of the existing version of the programme as well as the need to keep pace with changes in business and industry practices and requirements as the driving force behind this review. Each module was redesigned in order to address skill shortages identified in the information security industry as a whole while still addressing student academic development requirements at NFQ level 7 and 8 appropriate to a holder of a Bachelor of Science in Computing award. The panel queried if the redesign of the programme as proposed was largely focussed on the work based learner to the detriment of the full-time learner. However, following discussion with the redesign team it became apparent that the needs of the full-time learner would not only be met but they would benefit from the redesign by acquiring additional skill sets of immediate value to industry.

Electives were discussed, each confirmed as a standalone module with a minimum of 30 credits (2 ten credit mandatory modules plus one 10 credit elective module) to be taken per semester. The panel welcomed the design team's intention to offer electives online thus providing learners with the added opportunity of extending their knowledge base further. See panel recommendation VI.

A mapping diagram presented to the panel provided a visual linkage between the original ten 6 credit modules in years III and IV to the new structure comprising of six 10 credit modules in years III and IV. The panel queried the selection of modules dropped from the programme, in particular 'Leadership and Entrepreneurship'. The panel were informed of the opportunity learners have of attending business start-up seminars and workshops run on a monthly basis in the Institute's Learning and Innovation Centre (LINC) and also of how relevant subject matter has been incorporated into the 'Individual Project' module.

#### 7.5. Access, transfer and progression

The panel confirmed that the programme incorporates the established procedures for access, transfer and progression while accommodating a variety of access and entry requirements from applicants with expertise in this discipline.

### 7.6. Transition arrangements

The panel noted the omission within the documentation of transition arrangements with regard to students having to repeat modules no longer being offered in the proposed new version of the programme and requested that this be clearly defined. See panel recommendation I.

### 7.7. Industry certification

Through discussion the panel were informed of the various opportunities learners could avail of in acquiring industry certification as part of this programme in the areas of information security (CISSP<sup>3</sup>), forensics (ACE<sup>4</sup>) and networking (CCNA<sup>5</sup>). The panel was of the opinion that this built in added value to the programme could be better exploited from a marketing perspective. See panel recommendation III.

### 7.8. Legal and ethical considerations

The panel was informed of how these topics are integrated across multiple modules during the course of the programme. However, the panel recommended that their delivery be clearly defined in the learning outcomes and indicative content of the relevant modules. See panel recommendation IV.

### 7.9. Industry panel

The panel recommended the formal establishment of an industry panel not only to ensure the relevance of programme content in an ever evolving discipline but also to provide opportunity for guest lectures on areas of expertise currently not covered by departmental staff with eDiscovery<sup>6</sup> cited as an example. See panel recommendation V.

## 8. Meeting with academic staff:

### 8.1. Assessment

The panel stressed the importance of a programme assessment strategy and recommended that one be defined to provide clear guidance on the number and type of assessments per module and maximise the potential use of integrative assessments. The panel also pointed out the lack of definition within module syllabi regarding assessment events and requested that this

---

<sup>3</sup> 'Certified Information System Security Professional' - An industry certification reflecting the qualifications of information systems security practitioners.

<sup>4</sup> AccessData Certified Examiner - The ACE credential demonstrates proficiency with Forensic Toolkit technology

<sup>5</sup> Cisco Certified Network Associate - certification program for entry-level network engineers

<sup>6</sup> Electronic discovery – refers to discovery in civil litigation which deals with the exchange of information in electronic format

be addressed through Coursebuilder. The panel recommended that HETAC policy “Assessment and Standards” (2009), be referenced by all staff to provide guidance on best practice relating to assessment. The panel was also of the opinion that more integrative assessments could be used to strengthen the attainment of the programme learning outcomes.

## 8.2. Module titles, descriptors and indicative content

Concern was raised by the panel that the module titles, descriptors and indicative content as proposed do not accurately reflect the level of forensics within the programme. The panel recommended that the ‘Distributed Systems’ module title be revised and suggested the following:

‘Biometrics’ be renamed ‘Biometrics and Forensic Applications’  
‘Cloud Security’ be renamed ‘Emerging Security Technologies’

The panel also cited a lack of consistency within the documentation relating to the following:

- No of module learning outcomes
- Learning outcomes capture of higher order cognitive skills required of Level 7 and Level 8 modules
- Indicative content
- Coursework details (events and descriptors)
- Reference to independent learning
- Terminology of learning outcomes
- Linking of module learning outcomes to assessment events
- Resources (reading lists, internet based resources etc.)

## 9. Decision of the panel

The panel recommended all proposed changes for approval subject to the following specific condition and recommendations:

### 9.1. Condition

Revise and update as per Institute policy both programme and module information to accurately reflect and inform prospective learners and stakeholders whilst eliminating inconsistency and omissions relating to the following:

- Number and terminology of module learning outcomes
- Learning outcomes capture of higher order cognitive skills required of Level 7 and Level 8 modules
- Indicative content
- Coursework details (events and descriptors)
- Reference to independent learning
- Linking of module learning outcomes to assessment events
- Linking of module learning outcomes to the programme learning outcomes
- Resources (reading lists, internet based resources etc.)

### 9.2. Recommendations

- 9.2.1. Clearly articulate all transfer/transition arrangements for existing students, including repeats, transferring to the new curriculum.
- 9.2.2. Revise and be more creative with the module titles to more accurately reflect the forensic perspective of the programme . In particular, re-title the module ‘Distributed Systems’, ‘Biometrics’ be renamed ‘Biometrics and Forensic Applications’ and ‘Cloud Security’ be renamed ‘Emerging Security Technologies’.
- 9.2.3. Revise marketing material to better exploit the level of industry certification learners will have the opportunity of acquiring as part of this programme.
- 9.2.4. Clearly define and specify where relevant legal and ethical considerations will be covered in the learning outcomes and indicative content of modules.
- 9.2.5. Establish an industry panel not only to ensure the relevance of programme content but also to provide opportunity for guest lectures on areas of expertise currently not covered by departmental staff in an ever evolving discipline.

- 9.2.6. Fulfil the intention as discussed at the panel meeting of offering electives online.
- 9.2.7. Make other technical and minor amendments as discussed at the panel meeting.

## 10. Panel observations

The panel commended the design team on this initiative to respond to industry needs in an ever evolving discipline and the obvious dedication of staff to the ethos of continuous improvement. The panel was also of the opinion that this programme would produce highly employable graduates of immediate value to the information security sector.

## 11. Signatures

### Chair

Dr. Stephen Cassidy \_\_\_\_\_ Date \_\_\_\_\_

### Secretary

Dr. Diarmuid O'Callaghan \_\_\_\_\_ Date \_\_\_\_\_