FINAL ASSESSMENT REPORT
Executive Summary
Cyclical Program Review

Degree Program:	**Bachelor Of Information Technology (Hons), Networking and Information Technology Security**
Components:	**Internship**
Dean:	**Dr. Carolyn McGregor**
Date:	**May 13, 2025**

Under Ontario Tech University's Institutional Quality Assurance Process (IQAP) and the Ontario Quality Assurance Framework (QAF), all programs are subject to a comprehensive review at least/at minimum every eight years to ensure that they continue to meet provincial quality assurance requirements and to support their ongoing rigour and coherence.

In academic years 2021-2023 a program review was scheduled for the Bachelor of Information Technology – Networking and Information Technology Security program This is the second program review for this program. A timeline of the review is provided below.

Program Review Timeline	Date
Program Review start date:	November 17, 2021
Self Study submitted/approved:	November 22, 2023
Site Visit:	July 17-18, 2024
External Reviewers Report received:	December 6, 2024
Program Response received:	March 30, 2025
Decanal Response received:	April 5, 2025

Based on the self-study, the reviewers were asked to provide recommendations on program learning outcomes; program structure; experiential learning opportunities specific to the NITS program and generally available to FBIT students; laboratory

resources available to students; opportunities and challenges associated with a program in the ever-changing and ever-evolving field of IT.

The review consisted of two external reviewers. During the virtual site visit, the reviewers met with the following groups and individuals:

Dr. Lori Livingston, Provost and VP Academic
Dr. Carolyn McGregor AM, Dean, Faculty of Business and Information Technology
Dr. Mehdi Hossein-Nejad, Associate Dean, Academic Strategy
Dr. Brent MacRae (Chair of the Internal Assessment Team)
Members of the Internal Assessment Team
Faculty, Staff, and Students from the Faculty of Business and Information Technology

- The external reviewers identified 5 overall recommendations identifying specific steps to be taken to improve the program which included:
    - Creating appropriate mechanisms for ongoing market assessment and curricular review to keep pace with an ever-evolving field
    - Growing strategic partnerships and engagement with research community and industry in support of the program
    - Introduce industry grade security appliances (Fortinet)
    - Increasing faculty complement with expertise in cybersecurity certifications and tools
    - Enhancing available laboratory resources for students.

The prioritized list of recommendations is available in the Implementation Plan.

A Final Assessment Report (FAR) has been prepared to synthesize the reports and recommendations resulting from the review, identifying the strengths of the program as well as the opportunities for program improvement and enhancement. The Implementation Plan (IP) presents a timeline of the follow-up and resource requirements addressing the recommendations from the external reviewers' report. Both documents, accompanied by this Executive Summary (ES), were delivered to the appropriate standing committee of Academic Council (USC/GSC) and approved on **May 20, 2025**.

Governance	Document(s)	Type of review	Date
Faculty Council	IP	Feedback	May 6, 2025
Resource Committee	IP	Resource review	May 13, 2025
USC/GSC	FAR, ES, IP	Approval	May 20, 2025
Quality Council	FAR, ES, IP	QAF requirement	
Academic Council	ES, IP	For information	
Board of Governors	ES, IP	For information	
Corporate Website	ES, IP	QAF requirement	

Due Date for 18-Month Follow-up Report: **April 30, 2026**
Date of Next Cyclical Review: **2028-2030**

IMPLEMENTATION PLAN
28 April 2025
Bachelor of IT – Networking and IT Security
Program Review
Prepared by: Dr. Carolyn McGregor

The Implementation Plan is a critical outcome of the Cyclical Program Review process. The Dean solicits feedback on the Implementation Plan through Faculty Council and the plan is reviewed by the Provost, through the Academic Resource Committee (ARC), to examine resource implications and allocations. A Final Assessment Report (FAR) and Executive Summary are prepared synthesizing the program review reports and responses, following review of the Implementation Plan by the ARC. The plan proceeds through Ontario Tech's governance process and is posted on the corporate website.

Recommendation	Action Item(s)	Specify role of person responsible	Timeline for action and monitoring	Resource Requirements
Program Committee - Program and Curricular Review:				
The growing complexity of networking and security in future warrants continuous market assessment, competitive analysis, and	*The Program Director with support from the Dean will complete the following by the end of the 25-26 Academic Year:* *-Ensure adequate planning and structure is put in place for the NITS program committee.*	*Dean's Office, Program Director*	*To be completed and progress reported to the dean at the end of 25-26 academic year.*	*Information from the RO*

curriculum upgrade incorporating new concepts and technologies. *Form a committee of faculty members of the program to oversight the program holding at least one meeting every term.*	*- Work with the Registrar's Office (RO) to gather information for market assessment and competitive analysis.* *- Ensure that the program committee meetings are routinely scheduled by the program director in order to review market assessment and competitive analysis from the RO, and curriculum upgrade incorporating new concepts and technologies.*			
form a committee of faculty members especially from the key areas of networking and security, which should set up a framework of periodic review of curriculum for incorporating changes relevant to industry.	*-Discuss and recommend new concepts, topics, and technologies. Within our governance structure the recommended program and curriculum committee can be the same committee of all faculty in the NITS program who meet. Any items requiring approval can then proceed through governance to UEC, FC etc.*	*Program Director*	*To be completed and progress reported to the dean at the end of 25-26 academic year.*	*None*
Program strengths and weaknesses should be reviewed. *Competitive and threat analysis for the program should be performed.*	*-Lead the Program Committee in a review of strengths and weaknesses and a threat analysis leading to a report to the dean and an implementation plan to capitalize on program strengths and create strategies to mitigate risks relating to program weaknesses. This will build on the efforts already conducted as part of the cyclical program review.*	*Program Director*	*Report to the dean to be completed by end of 25-26 academic year*	*None*

Curriculum should have more coherence and depth. Courses on networking, computer science, and security should not run as separate streams rather more connections and cohesions should be built. The security curriculum should increase hands-on learning components of the courses to make them more relevant to industry and bring more depth to them.	*Examine the security curriculum and determine if changes are needed. The committee will also look into opportunities for integration of our networking and security content if possible. The current course offering do however provide students with exposure to these topics.*	*Dean's office* *Program Director*	*Committee to report on any potential opportunities by end of 25-26 academic year.*	*None at this stage.*
The new set of Program Learning Outcomes (PLO) has no PLO related to foundational and conceptual knowledge. The program should consider adding one PLO to cover this gap.	*Develop a new PLO as recommended. The PD to arrange for the Program Review Committee to make this update to the program's PLOs*	*Program Director*	*December 2025*	*N/A*
The lab work should be included in all courses, and it should be the standard feature of the curriculum. Given the potential growth of the program, it is recommended to expand the lab space and upgrade the lab equipment.	*Review of courses and their associated tutorial and lab components to evaluate the student learning opportunities beyond the lecture components for all courses. The PD will provide the Dean with a report of this review in order to determine future resourcing requirements.*	*Program Director* *DPO*	*Committee to report by end of 25-26 academic year.*	*Resources may be needed if lab expansion or upgrades required as a result of this review and consultation with the Provost will take place as required.*

Additional Recommendations:

The program should have at least one dedicated lab technician who can provide support for networking and security labs.	*FBIT has already received approval for a second technician that will enable the faculty to provide more technical support for the networking and security labs. The hiring search process for this position has already commenced.*	*Dean's office*	*In progress and should be completed within weeks.*	*Resource allocated*
Program advisory committee – The PAC should be reintroduced. It is important for keeping the program up-to-date and in aligned with the industry.	*The Dean will provide mentorship and guidance to the PD, to reestablish a program advisory committee (PAC) for this program as part of our strategy to establish/reestablish such committees for all our programs.*	*Dean's office* *Program Director*	*PAC to be formed and meet at least once by end of 25-26 academic year*	*Resources for hosting members of PAC on campus*
Research and industry engagement should be enhanced through building partnership with research institutions and industries, showcasing collaborative research and projects, and utilizing the opportunities especially in security.	*The Dean will provide mentorship and guidance to enable the PD for NITS to work with the Director of the Institute for Cybersecurity and Resilient Systems to grow strategic partnerships that are aligned with networking and security.* *Continue to leverage relationships with industry partners through well-established internships.*	*Dean's office* *Program Director* *Director of ICRS*	*Ongoing*	*Resources for hosting potential industry related events on or off-campus.*
The HRL should introduce industry grade security appliances such as Palo Alto or Fortinet. It should also provide access to commercial cloud security features.	*The PD and the Program Committee will work on a plan to introduce Fortinet content to the technical security courses and if needed, provide the updated course information to UEC for progression through governance.*	*Program Director* *Associate Dean*	*Committee to develop plan by end of 25-26 academic year and present to UEC if any course changes are required.*	*Lab equipment updates as needed*

Security faculty should be expanded with instructors with industrial experience. To fill the gap in the security area, faculty with direct, hands-on experience in industry-standard cybersecurity certifications and tools should be recruited.	*A new hire in Networking and IT Security has accepted their offer and will commence on 1st July, 2025. The new hire has direct, hands-on experience in industry-standard cybersecurity certifications and tools.* *The growth of high quality industry experienced sessionals is also a strategy of interest for the faculty . The Dean will work with the PD on a strategy to grow a pool of high quality industry experienced priority sessionals.*	*Dean's office* *DPO*	*July 1, 2025 for new TF hire* *Ongoing for sessional hirings*	*Resource allocated*

Recommendations not Addressed and Rationale

#	Recommendation not Addressed *(corresponding # from reviewers' report)*	Rationale
1.a	*The current teaching load of the PD should be reduced and the involvement of the PD in lab development and delivery should be minimized for the effective leadership.*	*The collective agreement outlines workload for TTT and TF faculty members and the stipend or course release for the program director role. A clear job description document has been created to outline all responsibilities for this role so that candidates for the PD position are aware of the responsibilities and commitments.*
2.c	*Curriculum update should be decoupled from vendor specific content development, for example,*	*Some of the content in a number of our NITS courses do align with widely recognized industry certification. This is a*

	currently the major driving factor for curriculum development are the two company-specific certification programs. The faculty members in the program are qualified and actively involved in networking and security research. They should be involved in curriculum development.	*decision the program has deliberately made to ensure the success of graduates on the job market and it has paid off. This does not however mean that faculty member expertise or research has not influenced our curriculum or course content. To the contrary, our faculty incorporate a substantial amount of foundational and original content in what they teach. The program is also able to pivot away from current industry alignments towards other directions if it ever decides to do so.*