BELLEVUE
COLLEGE

STATE BOARD FOR COMMUNITY AND TECHNICAL COLLEGES
FEBRUARY 2-3, 2022
PROGRAM PROPOSAL
BACHELOR OF APPLIED SCIENCE
CYBERSECURITY

BELLEVUE COLLEGE

TABLE OF CONTENTS

Cover Page — Program Proposal

Program Information

Institution Name: Bellevue College

Degree Name: BAS Cybersecurity

CIP Code: 11.1003 (Computer and Information Systems Security/Auditing/Information Assurance)

Name(s) of existing technical associate degree(s) that will serve as the foundation for this program:

Degree: AAS-T Network Services & Computing Systems

CIP Code: 11.0901

Year Began: 2012

Proposed Start Implementation Date (i.e. Fall 2014): Fall 2022

Projected Enrollment (FTE) in Year One: 24

Projected Enrollment (FTE) by Year: Fall 2022

Funding Source: State FTE

Mode of Delivery

Single Campus Delivery: Bellevue College main campus, Bellevue WA

Off-site: N/A

Distance Learning: Some courses will be hybrid, synchronous distance, or online.

Program Proposal

Please see criteria and standard sheet. ***Page Limit: 30 pages***

Contact Information (Academic Department Representative)

Name: Robert Viens

Title: Associate Vice President of Academic Affairs

Address: 3000 Landerholm Circle SE, Bellevue WA 98007-6484

Telephone: (425) 564-2442

Email: rob.veins@bellevuecollege.edu

Chief Academic Officer signature

The Program Proposal must be signed. To sign, double click on the signature line below.

X ______________________________

Chief Academic Officer

11/8/2021

Introduction

This proposal is for a free-standing Bachelor of Applied Science in Cybersecurity at Bellevue College. Bellevue College's Bachelor of Applied Science (BAS) in Information Systems and Technology (IST) degree first enrolled students in Fall 2013. This degree currently has a concentration titled Cybersecurity (prior to July 2021, Cyber Security and Systems Administration [CSSA]), along with concentrations in Artificial Intelligence (prior to July 2021, Business Intelligence) and Application Development. For those students seeking employment in the field of cybersecurity, the BAS IST degree title does not complement the concentration's core content. Also, having three unrelated concentrations in the current BAS IST degree limits the capacity to fully develop focused curriculum to best support student learning. Bellevue College is proposing to remove the Cybersecurity concentration, along with its core and general education courses, to create a new Bachelor of Applied Science (BAS) in Cybersecurity.

Bellevue College requires that every new program align with its mission, which states:

> Bellevue College is a student-centered, comprehensive and innovative college, committed to teaching excellence, that advances the life-long educational development of its students while strengthening the economic, social and cultural life of its diverse community. The college promotes student success by providing high-quality, flexible, accessible educational programs and services; advancing pluralism, inclusion and global awareness; and acting as a catalyst and collaborator for a vibrant region. (Last updated September 24, 2014)

Developing baccalaureate degrees is a fully integrated component of Bellevue College's strategic planning. "Applied Baccalaureate Development" is a president's cabinet-level priority, with goals assessed annually. At Bellevue College, Bachelor of Applied Science degrees are developed through careful consideration of the college's strengths, strategic enrollment goals, workforce needs, community demand, and sustainability of each proposed degree. In addition to continuing education, certificates, professional/technical degrees and transfer degrees, baccalaureate degrees are a means through which Bellevue College provides the level of education required by local employers and citizens. As the workforce entry level criterion shifts from a two-year to a four-year degree in multiple fields, Bellevue College assesses the need for applied bachelor's degrees to meet demand for highly skilled employees, and to ensure that area residents have access to the education wanted and that meets workforce needs.

In 2009, Bellevue College was granted accreditation by the Northwest Commission of Colleges and Universities (NWCCU) to offer baccalaureate degrees. The college currently offers twelve bachelor's degrees (list found here), eleven bachelor of applied science degrees and one Bachelor of Science degree, in Computer Science. Baccalaureate degrees play an important role in Bellevue College's commitment to provide high quality, flexible, accessible education programs and to strengthen the economic life of its diverse community.

The Bachelor of Applied Science Cybersecurity will continue to meet the expressed needs of community college students seeking access to a bachelor's degree. The program will advance the life-long educational development of its students by offering a seamless educational pathway that will provide new career and career advancement opportunities to individuals with technical associate degrees in cybersecurity-related fields. Historically, the associate's technical degree has not been transferable, which makes it difficult for graduates to progress to a bachelor's degree in their chosen field.

Bellevue College is working with the College's Accreditation Liaison Officer to make sure the appropriate steps are taken to ensure compliance with the Northwest Commission of Colleges and University standards.

The proposed program supports the college mission of providing high-quality, flexible educational programs and services that are academically, geographically, and financially accessible. Some courses will be offered in hybrid or online, and in the later afternoon or evening which will add to the flexibility for students with busy schedules. Tuition set at the regional baccalaureate rate means this degree will be more affordable for students than many other options.

Criteria 1

Curriculum demonstrates baccalaureate level rigor.

1.1 Program learning outcomes

Bellevue College has carefully designed the overall curriculum scope, as well as individual courses, to help students gain the knowledge, skills, and abilities needed to be successful cybersecurity professionals. Successful graduates of the program will meet all course and program learning outcomes.

The Bachelor of Applied Science (BAS) in Cybersecurity will provide students with a foundation of theoretical and technical knowledge in cybersecurity. This degree prepares graduates to monitor and maintain system security solutions, including legal, regulatory, and internal compliance solutions. Graduates will be able to translate security policy into technical architecture. In addition, this program prepares students for system administration tasks which include interoperation, automation, virtualization, and storage.

This degree completion program is designed for individuals with two-year degrees in networking or cybersecurity related fields.

Program graduates should be able to:

- Apply a broad understanding of Cybersecurity, creative problem-solving techniques and systems thinking to develop organizational solutions;
- Work effectively in multi-disciplinary teams to apply information technology in support of organizational goals;
- Identify and analyze user needs and take them into account in the selection, creation, evaluation, implementation and administration of technology systems;
- Work efficiently and effectively applying sound project management techniques and professional communication skills;
- Analyze the local and global impact of Cybersecurity on individuals, organizations, and society and apply sustainable business practices; and

- Apply best practices and standards, conform to legal and regulatory standards, and apply appropriate ethical considerations including respect for privacy, intellectual property.

1.2 Program evaluation criteria and process

Bellevue College uses a multifaceted approach to program review to ensure continuous improvement. Table 1 shows the multiple modalities used and what each modality assesses.

Table 1: Program Assessment

Effectiveness of curriculum/ program — continuously refines curriculum and program design, keeping the program current, including discipline-based, general education and electives	
Course evaluations by students- Quarterly	Effectiveness of curriculum & teaching methods in courses Effectiveness of program in skills & knowledge progression
Student survey and/or focus group mid-point through the program and at graduation- Annually	Effectiveness of the program in skills & knowledge progression Adequate balance of knowledge & skills, theory & practice Effectiveness of program in meeting students' expectations Effectiveness of institutional and program resources and support Preparedness of faculty Preparedness of students upon entering individual courses
Program Review- Every 5 years	Student retention Student course success Student progression through program Correlation of student success and training/job experience prior to entry
Program Viability- Annually	Enrollment rates Faculty/student ratio Financial data
Survey of BAS Cybersecurity program faculty- Annually	Preparedness of students upon entering individual courses Preparedness of students upon entering the program
Graduate follow-up and industry feedback — assesses effectiveness of program in meeting career goals and employer expectations and uses findings to refine curriculum and teaching methodologies	
Survey of program graduates- Quarterly	Effect of program completion on career Effectiveness of program in meeting job expectations Wage and career progression
Survey of employers of program graduates- Under Development	Effectiveness of program in meeting job expectations Observed increased skills and performance Perceived strengths and weaknesses of current program
Oversight by Advisory Committee – provides ongoing support and program review	
BAS Cybersecurity Program Advisory Committee – Twice a Year	Completeness & relevance of curriculum to employer needs Trends in field, technologies, practices and job markets
Survey of faculty satisfaction — assesses adequacy of program support and faculty training	
Survey of program faculty- Annually	Effectiveness of institutional & program resources & support Preparedness to teach the curriculum

Impact on two-year programs — assesses impact of BAS Cybersecurity program on existing degrees	
Survey and/or focus group of students enrolled in two-year degree programs- Annually	Impact of BAS Cybersecurity program on the quality of the 2-year degrees Impact on faculty availability and support Impact on institution & program resources & support
Survey of faculty teaching the two-year associate degree programs- Annually	Impact of BAS Cybersecurity program on the quality of the 2-year degree Impact on faculty availability and support Impact on institution & program resources & support

Assessment for the proposed Bachelor of Applied Science (BAS) in Cybersecurity program is based on the comprehensive student achievement and program assessment processes in place at Bellevue College for all programs, including associate and baccalaureate degrees. Program review occurs every five years and provides a thorough assessment of every aspect of the program. This peer-review process closely aligns with the College's core themes of Student Success, Teaching and Learning Excellence, College Life and Culture, and Community Engagement. The data-informed process asks the program chair and faculty to review key metrics on student success and enrollment, providing analysis and action plans for improvement.

In 2019 faculty and staff completed the college's 5-year program review. This review evaluated the BAS Information Systems and Technology (IST)- Cybersecurity program's effectiveness by collecting and analyzing data on student satisfaction, preparedness, and retention; faculty assessment of student preparedness; and effectiveness of courses to meet the program outcomes.

The program advisory committee provides an opportunity for college faculty to learn from and engage with industry leaders as these professionals review the curriculum and program elements on a regular basis. The advisory committee has been expanded from the current 2-year degree advisory committee in order to better serve the expanded outcomes and scope of the BAS Information Systems and Technology- Cybersecurity program. The role of this committee will be to advise the program on recommended curriculum improvements; help keep the program abreast of changes in the field; assist in student recruitment and placement; and make recommendations for other changes that will keep the program current.

1.3 Course preparation needed by students transferring with technical associate degree

The BAS Cybersecurity has been designed for individuals who have earned a professional technical associates degree in a networking or cybersecurity-related area.

In addition to holding a technical associate degree in a networking or cybersecurity-related area, applicants to the BAS Cybersecurity will need to meet the minimum requirements outlined in Table 2 below. In keeping with the open access mission of the community college, admission requirements have been designed to provide access to many and to ensure that prospective applicants are prepared for success upon entering the program. Students with technical degrees in networking or cybersecurity are well prepared for the BAS Cybersecurity.

Table 2: BAS Cybersecurity Eligibility

BAS Cybersecurity Eligibility	
Students may be admitted with an associate degree in IT or CS-related field or with 65 equivalent credits that represent the combination of program admission required courses and other college-level credits.	
Eligibility	• Cumulative GPA of 2.0 or higher, with a minimum grade of C in all prerequisite courses. • At least 20 credits of general education requirements completed as part of the associate's degree. • Technology or math credits must not be more than 5 years old. Math classes more than 5 years old may be accepted based on Math placement test results (see program advisor).
Technical Prerequisites 45 Credits	• IT 128 - Information Security Essentials 5 CR • IT 223 - Using & Supporting Linux 5 CR • NSCOM 201 - CISCO Networking I 5 CR • NSCOM 202 - CISCO Networking II 5 CR • NSCOM 203 – CISCO Networking III 5 CR • NSCOM 231 – Introduction to Cloud Architecture and Services 5 CR • NSCOM 235 – Cloud Infrastructure 5 CR • NSCOM 240 – Cloud Services 5 CR • PROG 108 – Intro to Scripting 5 CR
Program Prerequisites (General Education) **20-21 Credits**	• ENGL& 101 - English Composition I 5 CR • ENGL 201 - The Research Paper or ENGL& 235 - Technical Writing or ENGL 271 Expository Writing 5 CR • At least five credits must be in physical, biological, and/or Earth sciences from AAS-DTA Natural Science list. Shall include at least one laboratory course 5-6 CR • MATH 138 - College Algebra for Business & Social Science 5 CR or higher

1.4 General education component

Bellevue College has planned carefully to ensure that general education credits and courses meet state guidelines for general education within applied baccalaureate degrees. Over the course of the degree, the state requires that general education credits include a minimum of ten credits of written communication skills, including English composition; five credits of quantitative skills; ten credits of humanities; ten credits of social science, and ten credits of natural science, including at least one life sciences course and one course with a lab.

All BAS Cybersecurity degree graduates will have taken 60 credits of general education. Thirty credits of which are typically satisfied at the associate-degree level as confirmed by entrance prerequisites. See Appendix A for list of general education courses included in the Bellevue College AAS-T (Associate in Applied Science-T) Degree Network Services and Computing Systems (NSCOM).

Bellevue College plans to work closely with other system colleges to ensure that students currently enrolled in technical associate degrees take appropriate general education courses prior to graduation and admission into the BAS Cybersecurity. The remaining 30 credits are satisfied at the upper division level by courses in philosophy, business, communication studies and general education distribution courses.

General education requirements in the Cybersecurity degree are outlined in Table 3 below. Courses annotated with an asterisk will be completed as part of the AAS-T degree. Course numbers with an ampersand symbol (&) are common course numbers at all Washington State community and technical colleges. Course numbers without the ampersand symbol refer to Bellevue College Courses.

Table 3: General Education Components

Course	Title	Credits
*ENGL& 101	English Composition I	5
*ENGL 201, *ENGL& 235, or *ENGL 271	The Research Paper Technical Writing Expository Writing I	5
Communication Total		10
*MATH 138 or higher	College Algebra for Business & Social Science	5
Quantitative Skills Total		5
CMST 340	Advanced Communication in Business & Technology	5
PHIL& 115	Critical Thinking	5
Humanities Total		10
*BUS& 101	Introduction to Business	5
200 level Social Science		5
Social Sciences Total		10
*PHYS 109	Science for Information Technology	6
Natural Science course		5
Natural Sciences Total		10-11
CMST 250	Communication in a Diverse Workplace	5
PHIL 375	Ethical Issues in Information Technology	5
BUS 355	Business of IT	5
Other Total		15
TOTAL REQUIRED		**60-61**

1.5 Course work needed at junior and senior levels in the baccalaureate program.

The BAS Cybersecurity is being designed with working students in mind. Courses will be taught in the evening or through a hybrid model in which degree candidates spend some class time face to face with the instructor and some class time online. All students take the core courses in cybersecurity, as well as general education courses in communication studies, business, and philosophy. Full course descriptions for the BAS coursework are listed in Appendix B.

Total program credits are 180, 65 of which are met by entry requirements. For reference, the Bellevue College AAS-T (Associate in Applied Science-T) Degree in NSCOM is included in Appendix A to give an example of the coursework the two-year graduates will have completed prior to entering the BAS program. Graduates coming from other colleges may have completed a different set of courses. BAS program staff will work with each student to develop pathways into the BAS program based on their education background.

Table 4: Bellevue College BAS Cybersecurity Degree Requirements

Courses	Credits
ISIT 300 - Problem Solving Strategies	5
ISIT 305 - Network Security and Firewalls	5
ISIT 312 - Project Management for IT	5
ISIT 344 - Virtualization & Storage	5
ISIT 350 - Digital Forensics	5
ISIT 440 - Administering a Linux Server	5
ISIT 444 - Automation/Configuration & Management	5
ISIT 450 - Network Vulnerabilities and Countermeasures	5
ISIT 452 - Network Security Monitoring	5
ISIT 454 - System Hardening	5
Pick one set ISIT 490 - ISIT Capstone I and ISIT 491 - ISIT Capstone II or EXPRL 490 - Internship Experience and EXPRL 491 - Internship Experience	10
Total Core Applied Technology Courses	60
BUS 355 - Business of IT: Legal Regulatory Business Environment	5
CMST 340 Applied Org Communication	5
PHIL& 115 - Critical Thinking	5
PHIL 375 - Ethical Issues in Information Technology	5
Natural Science course in physical, biological, and/or Earth sciences or math from AAS-DTA Natural Science list	5
Any 200-level Social Science course from AAS-DTA transfer list	5
Total General Education Courses	30
Total BAS Coursework	**90 credits**

Students attending full-time (which is typically three courses or 15 credits each quarter) finish the program in six quarters. Students attending part-time finish the program in nine quarters or more, depending on the number of credits carried each quarter.

Program faculty and the program manager will work with each student to develop an academic plan, ensuring that full-time and part-time students are able to efficiently meet their degree and career goals. An example of a full-time schedule is in Table 5.

Because work experience is a key part of developing a career, students in the BAS Cybersecurity have the opportunity to complete a capstone course in their last two quarters in the program. Students may choose to do an internship as part of their capstone project.

Table 5: Sample Full-time BAS Cybersecurity Student Schedule

First Year (Junior)		
Fall	**Winter**	**Spring**
ISIT 305 Network Security and Firewalls	ISIT 350 Digital Forensics	ISIT 454 System Hardening
ISIT 440 Administering a Linux Server	ISIT 312 Project Management for IT	ISIT 344 Virtualization & Storage
ISIT 300 Problem Solving Strategies	PHIL& 115 Critical Thinking	Natural Science
Second Year (Senior)		
Fall	**Winter**	**Spring**
ISIT 450 Network Vulnerabilities and Countermeasures	ISIT 452 Network Security Monitoring	ISIT 444 Automation/Configuration & Management
200 level Social Science	PHIL 375 Ethical Issues in Information Technology	BUS 355 Business of IT: Legal Regulatory Business Environment
CMST 340 Advanced Communication in Business & Technology	ISIT 490 ISIT Capstone I	ISIT 491 ISIT Capstone II

Criteria 2

Qualified faculty.

Bellevue College faculty are highly qualified to teach within the proposed program.

(See the table below.)

Table 6: Qualified Full and Part Time Faculty

Full Time Faculty	
Faculty Name	Qualifications
Thomas Lee	• BS in Technology • 12 years of collegiate teaching • 20 years of technical work experience • Industry certifications: CompTIA A+ & CompTIA N
Diane Walser	• Associate of Technical Arts in Computer Information Systems – Network Technology BA in French • 13 years of collegiate teaching experience • 20 years of technical work experience

	• Industry certifications: CompTIA A+, CompTIA Network+, CompTIA Security+, CCNA, CCIA in CCNA and Cyberops
Part Time Faculty	
Faculty Name	Qualifications
Peter Ophoven	• MS Creativity and Innovation in the school of Education • 7 years of collegiate teaching experience • 31 years of technical work experience • Industry certifications: ITIL, Pop Fiction, Private Investigations, Forensic Sciences, MBE - Mind Brain and Education, Foursight Assessment, Google Analytics, Scrum Master
Andrew Hunt	• Master's in Education • 6 years of collegiate teaching experience • 25 years of technical work experience • Industry certifications: CISA, Azure Administrator
Anand Injeti	• MBA with Technology Management Focus • 20 years of collegiate teaching experience • 25 years of technical work experience • Industry certifications: Checkpoint and PaloAlto Certifications in Firewalls and Intrusion Protection and Detection
Chris Kacoroski	• MS in Physics • 20 years of collegiate teaching experience • 36 years of technical work experience

The full time faculty listed above share appointments with Cybersecurity and other disciplines. Bellevue College Institute for Business and Information Technology division will be recruiting for additional full-time faculty, with the following qualifications (core competencies):

- Bachelor's degree from a regionally accredited institution in Information Technology or related field.
- Applicable industry certifications.
- Substantial, recent full-time experience in the industry and/or teaching experience in Cybersecurity, Networking, Network Security, Systems Administration, and related areas.
- Demonstrate commitment to working with students and colleagues from diverse backgrounds and academic readiness.

In addition to the above qualifications, preferred qualifications will include, but are not limited to:

- Experience in cybersecurity. Such as, but not limited to, forensics, incident response, OS hardening, penetration testing, etc.

- Experience with management, administration of virtualized hardware such as VMware or Hyper-V environments.
- Must possess or obtain certifications such as CompTIA Security+, CISSP, CHFI, GSEC, CCNA CyberOps and AWS Solution Architect within 2 years of hire date.

Faculty who teach the general education requirements for the BAS Cybersecurity are also highly qualified within their disciplines (see Table 7).

Table 7: General Education Full-Time Faculty Profiles

Faculty Name	Degree	Distribution Area
Stephanie Hurst	MA	Communication Studies
William Russ Payne	Ph.D.	Philosophy
Frank Hatstat	JD, MBA	Business

Criteria 3

Selective admissions process, if used for the program, consistent with an open-door institution.

Although the proposed degree will employ a selective admissions process, it will be consistent with the college's open-door philosophy. The 2.0 GPA requirement is consistent with it's the required GPA for two-year progression. This qualification has been evaluated each year and in the last program review, in 2019. Students who come in with an overall 2.0 GPA, have been found to be successful in the program. Qualified applicants who meet the priority application due date will receive first consideration. If there are more program slots than applications, applicants who do not meet the priority application date will be considered. The program manager and program faculty will manage the details of the admission process.

Should there be more qualified applicants than there are openings in the program, the college will first consider offering additional course sections, if feasible. For example, if there were 50 qualified applicants and 25 openings, the college would consider adding a cohort, if appropriate faculty are available, so that all qualified students would be admitted.

If there are more qualified applicants than there are openings, but not enough applicants to add an additional section, or another section is not feasible, the college will admit some students and place the remainder on a wait list, based on the following criteria:

- Fifty-percent of the cohort slots will be awarded based on GPA, rank ordered, i.e., 3.8, 3.78, 3.6. This provides priority to students with a higher GPA.

- The remaining fifty percent of cohort slots will be awarded by lottery, from the remainder of qualified applicants. This ensures that students with passing but not exceptionally high GPA are not excluded from admission.
- Any remaining qualified applicants will be placed on a wait list.
- If additional program slots become available, admission will be determined by lottery from the wait list, so all students will have equal opportunity to be admitted.

The program will assess this process each year and determine if changes need to be made, based on student progress and retention, diversity of student group, and other factors which may emerge.

The bachelor's program will employ practices implemented by the college's Office of Diversity, Equity and Inclusion to attract a diverse student population to the college. These include:

- Recruit people of color who are BC program graduates and professionals to serve as role models, serve on the advisory committee and make presentations to currently enrolled associate degree students to encourage the pursuit of a bachelor's degree;
- Engage in targeted marketing and other marketing efforts to encourage persons of color and those from underserved populations to apply to the program;
- Coordinate program diversity efforts with the institution's office of Multicultural Student Services;
- Apply best practices for identifying potential hires from underrepresented groups;
- Work with businesses and professional organizations to develop additional strategies to attract a diverse student body from workers in their employment ranks who do not have a bachelor's degree; and,
- Regularly assess recruitment/retention efforts with regard to underrepresented populations, and continually monitor and strive to improve the program's culture of appreciation and respect towards diversity.

Criteria 4

Appropriate student services plan.

As a community college, one of Bellevue College's strengths is the variety of student-focused support services that help students achieve success and accomplish their goals. Students in the Bachelor of Applied Science Cybersecurity program will be supported by the same high-quality student services that all students receive.

As Bellevue College has added new applied baccalaureate degrees, the college has focused on integrating support for baccalaureate students across the institution. For example, additional FTE have been added in enrollment services to provide transcript evaluation for incoming applied-baccalaureate students. Beginning in academic year 2013-14, the library has added 1 FTE librarian assigned specifically to the bachelor's degree programs, providing another institutional touch point for students.

Data has shown, at least 50% of students in the current BAS Information Systems and Technology (IST) Cybersecurity concentration are working and may have needs for alternative scheduling. Since 2013 security classes have been offered in evening or hybrid-delivery classes. In order to ensure access to program advising, the program manager or program chair is available for evening appointments, in addition to availability by email and Teams messaging. The program manager is the primary point-of-contact for students, from before admission, through the program, and into transition to master's degrees for those who wish to continue to graduate school. This primary-point-of-contact model has worked well in Bellevue College's other applied baccalaureate degrees, and the college plans to continue it for future degrees.

To provide convenient access to all students, Bellevue College has numerous services available electronically, including: quarterly online registration; online tutoring; 24/7 access to librarians through "ask a librarian"; extensive research databases suitable for baccalaureate-level research; and degree audit and transcript requests.

For face-to-face connection with all students, many services have evening and/or weekend hours, including: the academic success center, math lab, writing lab, computer labs, science study center, counseling center, financial aid, the library and extended testing hours at the disability resource center.

The following services will be those most frequently used by baccalaureate students.

Student Advising: The model that has worked well for the college's baccalaureate programs and will be used for the proposed degree is an embedded program manager who works one-on-one with students to facilitate their success. The program manager assists students with their educational planning and progress towards degree completion. The program manager and program chair consult regularly about each student's progress. Each student will have an individualized schedule and advising plan. Students can use online advising services and degree planning worksheets to access their information. The online degree planning tool helps faculty advisors and students evaluate, monitor and track the student's progress toward completion of a degree. Student retention and success are the college's top priorities. Students appreciate and respond well to having a specific person to go to for assistance. Program faculty will work with students who need additional assistance to develop personalized student success strategies.

Academic Success Center (ASC): The Academic Success Center assists students with successfully completing their college courses through one-on-one and group tutoring, workshops, classes, and open labs in reading, writing and math. As needed, additional tutors in the Academic Success Center, will be hired to meet the needs of students in higher-level Bachelor of Applied Science courses

Computer Labs: Bellevue College provides a wide variety of specialized computer labs to enhance learning and student success as well as a 200-computer open lab.

Credentials Evaluation: Full-time credentials evaluators have extensive experience evaluating transcripts from accredited institutions. Incoming students are evaluated for compliance with admission requirements and student records for all degree requirements when students near graduation. Bellevue College is committed to providing efficient time-to-degree for students, and makes every effort to accept prior learning when appropriate.

Disability Resource Center (DRC): The DRC provides assessment and accommodations for students with documented disabilities. Services provided include special course materials; testing coordination for disabled students and faculty assistance to provide appropriate accommodation.

Financial Aid: The financial aid office prepares and disburses federal, state, and institutional aid for all Bellevue College students. Students can monitor the progress of their application online.

Job Placement: Providing help with career advancement and job placement will be priorities for this program. An effective advisory committee comprised of regional cybersecurity employers will help to identify jobs. Through the internship or capstone course, students will develop potential job contacts. The Center for Career Connections has been successful in helping students find jobs by providing career planning and job placement assistance and conducting career fairs. The Center for Career Connections, Program Chair, and Advisory Committee will work closely to develop and nurture internship and job placements.

Multicultural Student Services (MCS): Multicultural Student Services offers advising, mentoring, tutoring, emergency financial assistance, and support for the college's multicultural student population.

Online Services: All students have online access to the bookstore, records and grades, registration, advising, faculty communication, and library services. As an example of integrated services, the library has added extensive online collections and resources. Library faculty have also developed upper-division research workshops for students in applied baccalaureate programs. The distance education office provides extensive technology assistance and student services for all online students.

TRiO: Students who are first-generation college, low-income, or have a documented disability receive academic and personal support through TRiO. Services include tutoring, study skills, advocacy, and laptop computer lending. The Department of Education has approved extension of this program to all bachelor's degree students who fit eligibility criteria.

Veteran's Administration Programs: The Veterans Affairs Office assists all eligible veterans, reservists, dependents, and VA chapter 31 students. Bellevue College has recently hired a Director of Veteran's Office to better support out veterans and their families.

Workforce Development: Bellevue College's Workforce Education department helps people get the skills they need through professional-technical programs to enter or re-enter the workforce. The Bachelor of Applied Science Information Systems and Technology Cybersecurity degree is an approved workforce program. Workforce funding sources include BFET, Opportunity Grant and Worker Retraining.

Criteria 5

Commitment to build and sustain a high-quality program.

5.1 Types of funds to be used to support the program

The Bachelor of Applied Science Cybersecurity will be funded by state tuition and fees.

5.2 & 5.5 Projected Program Expenses and anticipated revenue

	Year 1	Year 2	Year 3	Year 4	Year 5
Projected Revenue					
Tuition[1,2]	$376,427	$416,298	$460,392	$513,871	$573,563
Course Fees	$16,654	$18,406	$20,332	$22,656	$25,234
Total Revenue	$393,080	$434,704	$480,724	$536,527	$598,797
Projected Expenses					
F/T Faculty Salaries[3]	$74,241	$76,468	$78,762	$81,125	$167,118[4]
P/T Faculty[3]	$45,765	$47,138	$63,118	$65,011	$30,905
Exempt Employees	$61,020	$62,815	$64,736	$66,678	$68,679
Employee Benefits	$56,118	$57,802	$64,051	$65,973	$82,678
Goods & Services	$1,810	$1,865	$2,066	$2,128	$2,667
Hardware/Software	$905	$932	$1,033	$1,064	$1,334
Travel & Conf	$2,715	$2,797	$3,099	$3,192	$4,001
Total Expenditures	$245,575	$249,852	$276,866	$285,172	$375,380
Balance	$150,506	$184,852	$203,858	$251,356	$241,416
%Margin	62%	74%	74%	88%	68%

1. assume two initial 24 person cohorts with 7%-10% progressive growth
2. assume 2.8% tuition increase year 1. 2.4% increase thereafter
3. assume a year one 1.7% COLA. 3% COLA thereafter
4. second full-time faculty added to address growth and maintain 1:28 faculty to student ratio

5.3 Appropriate Facilities

The Bellevue College campus is a wooded 120 acres. The campus landscape is enhanced by more than 20 buildings, including two Gold LEED certified buildings. There are four computer labs dedicated to students in the Institute for Business and Information Technology, the division in which this BAS resides. There is a dedicated BAS librarian who provides services for BAS students and faculty.

5.4 Appropriate equipment, technology, and instructional resources needed for the program

The facilities, equipment, technology, and instructional resources needed for the program are currently in place for the AAS-T Network Services and Computing Systems and the current Bachelor of Applied Science Information Systems and Technology programs. Much of the hardware and software was recently updated to meet the current curriculum needs.

Utilization of the current dedicated classroom/lab space will continue to support the Bachelor of Applied Science Cybersecurity program. A move to remote operations due to Covid has been required over the past year, This shift in modality has opened up new opportunities for instructors to develop online content that can be used in conjunction with on-site projects moving forward. The library includes a dedicated librarian for the BAS programs who has a dedicated budget for obtaining appropriate BAS level library resources.

5.6 Document the college's ability to sustain the program over time

The Bachelor of Applied Science Cybersecurity serves students seeking employment in high demand career fields throughout the greater Seattle area, and beyond. The security industry's need for candidates with bachelor's credentials in the skillset provided by Bellevue College's Bachelor of Applied Science Cybersecurity has been steadily increasing as security breaches and risk reduction become top business concerns.

The college has been very supportive of this successful program by providing program managers, equipment, dedicated classroom space, and qualified faculty. Additionally, the college has provided marketing and recruiting resources leading to steady growth. Based on area demand for graduates, and the financial projections outlined in the 5.2 expenses and revenue table, the program is highly sustainable.

Criteria 6

Program specific accreditation.

Bellevue College had accreditation for the twelve bachelor's degree programs through the Northwest Commission of Colleges and Universities (NWCCU). Staff are working with the College's accreditation liaison officer to ensure that the BAS Cybersecurity will be appropriately accredited by NWCCU as well.

The cybersecurity profession prides itself on the quality of education offered to students and concerns itself with how well students will be able to perform in industry after graduating. If, at some point in the future, an appropriate program specific accreditation becomes an advantage for the BAS Cybersecurity and their graduates, the college will assess the potential benefits.

Criteria 7

Pathway options beyond baccalaureate degree.

Graduates of the BAS Cybersecurity who are interested in continuing their education will be well prepared to move forward into graduate schools.

While all BAS graduates can apply to any Master’s degree program, certain institutions offer graduate programs that continue the pathway of the Bellevue College Bachelor of Applied Science Cybersecurity graduates. These include:

- WGU: Cybersecurity and Information Assurance; and
- UW Tacoma: Master’s in Cybersecurity and Leadership.

These programs have been identified as Master’s degree options for which graduates of Bellevue College’s Bachelor of Applied Science Cybersecurity meet the declared prerequisites.

Criteria 8

External expert evaluation of program.

The reviewers for this proposal are Dr. Yan Bai, Ph.D, University of Washington Tacoma, Director of Cybersecurity and Leadership Master’s program and Dr. Erik Fretheim, Ph.D, Retired Colonel of the US Army Reserves and Professor of the US Military Academy at West Point, currently the Program Director of Cybersecurity at Western Washington University.

Response to their feedback.

Dr. Bai’s feedback was overall supportive of the Bellevue College Bachelor of Applied Science Cybersecurity degree proposal. There were positive comments in regard to meeting workforce needs and covering pertinent knowledge areas of Cybersecurity. Dr. Bai suggested additional mapping of course outcomes to program outcomes. This will be addressed during the process of obtaining NIST/NICE accreditation for the Bachelor of Applied Science Cybersecurity Program which has been identified by faculty as a future goal. Dr. Bai did express concern that the need for the Bachelor of Applied Science Cybersecurity Degree was not clearly stated and demonstrated. This information is present in the Statement of Need document.

Dr. Bai asked for revision of the Criteria 7 section in which pathways to master’s programs were highlighted. That section has been revised to state that graduates of the Bellevue College Bachelor of Applied Science program meet the stated prerequisites to apply for certain Master’s programs to further their Cybersecurity studies. Bellevue College faculty are in the early phase of articulation discussions with University of Washington Tacoma’s Masters of Cybersecurity and Leadership program and are hopeful that an articulation pathway will eventually be developed.

Additionally, Dr. Bai and Dr. Fretheim stated that there was lack of information regarding the role of the Advisory Committee. That piece was added to section 1.2 of the proposal accordingly. Both reviewers made note of what they view as possible deficiencies in faculty. Dr. Bai noted that no one faculty member is credentialed to teach all courses in the Bachelor of applied Science Cybersecurity program and Dr. Fretheim noted that many of the faculty lack relevant higher education degrees. This degree is an applied bachelor program, and in keeping with that principle, faculty who have strong industry experience have been chosen. Additionally, the program places an emphasis on diversity and relatability in faculty who, in turn, provide a diverse student population with resources for networking and connections to major industry. These connections are starting points for students to obtain gainful employment in the cybersecurity field.

Dr. Fretheim's primary suggestion, mentioned in several sections of the review document, revolved around outcome mapping and subsequent accreditation by governing bodies in the security industry. Obtaining accreditation from organizations such as NIST/NICE have been identified as goals by the program faculty. Developing Bachelor of Applied Science Cybersecurity program as a stand-alone degree is the first step towards the eventual goal of incorporating industry recognized accreditation and the program does intend to seek these credentials. Additionally, Dr. Fretheim recommended adjustment to program outcomes to remove redundancy and increase manageability. These changes have been made. Outcomes one, eight, and ten were removed and outcomes six and nine were combined. Individual course outcomes have been written as generally as possible and as technology evolves, the courses and outcomes will be updated as needed.

Dr. Fretheim identified several topic areas or outcomes that may not have been addressed sufficiently. These include risk management, programming, identifying and analyzing user needs, digital forensics, and system hardening. The concepts of risk management are introduced in ISIT 300 Problem Solving Strategies. Risk Management is assessed in ISIT 450 Network Vulnerabilities and Countermeasures, as response mechanism to risk analysis. In keeping with current job postings in the cybersecurity field, and the recommendation of the advisory board, Python scripting was added as a required class in the program. The faculty and advisory board will continue to review the need for additional programming courses in the degree. The outcome for identifying and analyzing user needs is addressed in a combination of ISIT 300 "Present concisely the problem and solution to an appropriate client," and ISIT 490/491 "Working productively in a team, and discuss issues using a constructive approach." The Advisory Board has identified the principles and application of digital forensics as an area of knowledge and ability sought by employers. Current trends in corporate security breaches mean that security professionals need a familiarity with the legal aspects of computer forensics and best practices for incident response. ISIT 350 Digital Forensics provides a foundation of knowledge, skills, and abilities for which students can obtain employment and through on the job training, build strength in this area. The system hardening topics in ISIT 454 are introduced in several previous courses. Those distributed topics are then concentrated and focused in ISIT 454 where students appraise and justify security methodologies in order to design and develop hardened systems for a deeper understanding. This escalation of skills throughout the program enhances employability.

Dr. Fretheim expressed concern that the credit loads for individual courses were too high and that there was not enough flexibility in general education requirements to "broaden students' perspectives". In regard to credit load, 5 credit courses are the standard credit load at Bellevue College which operates on the quarter system. While there are some program specific general education classes, students take a total of 60 credits of general education classes. Across the associate degree and the bachelor's degree we feel that students get a broad range of knowledge in classes such as PHIL 115 Critical Thinking; CMST 250 Communication in a Diverse Workplace; and 10 credits of Natural Science classes. The fact that this proposal is for an applied Bachelor of Science program also addresses Dr. Fretheim's concern that students may face theoretical shortfalls when pursuing technically focused graduate programs. The goal of this degree is to provide students with employable knowledge, skills, and abilities in the field of Cybersecurity.

Commendations were offered by both Dr. Bai and Dr. Fretheim:

- The Bachelor of Applied Science in Cybersecurity at Bellevue College will address the needs of cybersecurity workforce development. The curriculum and technical courses cover important domains of cybersecurity.
- The program outcomes are well designed, and will be assessed from various perspectives of different stakeholders. However, it would be better to add some detailed info for mapping different BAS in Cybersecurity courses to program learning outcomes.
- The program is well designed to provide students with technical knowledge in Cybersecurity, and will address cyber workforce needs. The proposal has good program evaluation criteria for different stakeholders.
- Really good that the program includes Project Management. That was a good choice.

Bellevue College thanks Dr. Bai and Dr. Fretheim for their time and effort in reviewing and providing highly constructive feedback for the improvement of the Bellevue College Bachelor of Applied Science Cybersecurity Degree.

Conclusion

Bellevue College is excited to build on our existing Cybersecurity concentration and create a stand-alone Bachelor of Applied Science which has been requested by students and employers to better serve both needs. The degree will continue to be a pathway for both Bellevue College students and students from other community colleges. We currently have an articulation agreement for our Bachelor of Applied Science Information Systems and Technology Cybersecurity degree with Edmonds Community College and are actively working to develop more articulation agreements with other area colleges. The field of cybersecurity is growing and developing a stand-alone degree will facilitate our ability to stay current with industry trends and incorporate them into the curriculum. Most cybersecurity related jobs require, at minimum, bachelor's degree. This degree will continue to provide students with access to living-wage jobs across the state and provide a path for students to continue into Master's degree programs. Thank you for your consideration of this reimagined degree option to support students who seek employment in the cybersecurity industry.

Appendix A: Bellevue College AAS-T Degree in Network Services and Computing Systems

Associate in Applied Science-T Degree Network Services and Computing Systems- AAS-T

Brief Description

The Network Services and Computing Systems Associate in Applied Science-Transfer degree addresses how to connect computers and other resources in a network, perform network maintenance tasks, and install and configure hardware and software. In addition to technical content, the degree includes skills in communication (oral, written, and listening), general business, teamwork, and problem-solving.

Learning Outcomes

Degree recipients should possess the skills & abilities described below:

- Write, speak, and listen effectively.
- Apply critical thinking and logical research to technological problems in area of concentration.
- Explain fundamental networking theory, terminology, and industry recognized standards.

Table 8: NSCOM AAS-T Requirements

COURSE NUMBER	COURSE NAME	CREDIT
BUS& 101	Introduction to Business	5
CMST 250	Communication in a Diverse Workplace	5
ENGL& 101	English Composition I	5
ENGL& 235	Technical Writing	5
IT 115	PC Analysis & Configuration I	5
IT 117	PC Analysis & Configuration II	5
IT 128	Information Security Essentials	5
IT 223	Using & Supporting Linux	5
IT 293	Technical Support Internship I **This needs to be completed at 4 CR for the degree*	1-6
MATH 138 or higher with a C or better	College Algebra for Business & Social Science	5
NSCOM 201	CISCO Networking I	5
NSCOM 202	CISCO Networking II	5
NSCOM 203	CISCO Networking III	5
NSCOM 231	Introduction to Cloud Architecture and Services	5
NSCOM 235	Cloud Infrastructure	5
NSCOM 240	Cloud Services	5
PHYS 109	Science for Information Technology	6
PROG 108	Introduction to Scripting	5
TOTAL		90

Appendix B: Course Descriptions

ISIT 300 Problem Solving Strategies – 5 credits

This course classifies and examines a variety of problem-solving methodologies to improve a person's problem solving and decision-making skills. Students engage in personal and group dynamics, vertical/convergent methods, creative/lateral thinking techniques and communication skills to apply and solve technical and non-technical problems.

Prerequisite(s): Permission of instructor.

Course Outcomes

- Apply problem-solving skills in today's organizations.
- Distinguish, develop, and classify problem-solving strategies in individual and group settings.
- Analyze and articulate causes of a problem.
- Present both the problem-solving process and defend the effectiveness of the outcome.
- Articulate problem-solving strategies and methodologies in relation to organizational problems.
- Experiment with lateral and vertical thinking techniques to arrive at a solution.
- Present concisely the problem and solution to an appropriate client.
- Compile and implement a plan to use technology in problem-solving.

ISIT 305 Network Security and Firewalls – 5 credits

This course covers the skills required to develop a security infrastructure, recognize threats and vulnerabilities to networks, and mitigate those threats. Emphasizes core security technologies, installation, troubleshooting and monitoring of network devices to maintain integrity, confidentiality and availability of data and devices. Includes attack and defense case study.

Prerequisite(s): NSCOM 202 or permission of the instructor.

Course Outcomes

- Describe common security threats with appropriate countermeasures.
- Implement security on Cisco routers and switches.
- Describe, implement, and verify Authorization, Authentication and Accounting (AAA) on devices.
- Describe and implement secure network management practices.
- Evaluate operational strengths and weaknesses of the different firewall technologies.
- Implement the Cisco Adaptive Security Appliance (ASA).
- Assess the applicability of the different methods used in cryptography.
- Implement an Internetwork Operating System (IOS) Internet Protocol Security (IPSec) site-to-site Virtual Private Network (VPN) with pre-shared key authentication.

ISIT 344 Virtualization & Storage – 5 credits

This course introduces and applies the concepts of design, implementation, management and troubleshooting of server virtualization, network virtualization and large storage systems. Technologies include VMware and Storage Area Networks (SAN) solutions.

Prerequisite(s): NSCOM 202 or permission of the instructor.

Course Outcomes

- Install and configure ESXi.
- Install and configure vCenter Server components.
- Configure and manage ESXi networking and storage using vCenter Server.
- Deploy, manage, and migrate virtual machines.
- Describe the architecture of a Data Center environment with RAID and Intelligent Storage Systems.
- Configure and manage a SAN.
- Describe a system backup and restoration.
- Configure replication of data.
- Configure security through best practices.

ISIT 350 Digital Forensics – 5 credits

Introduces students to computer forensics, both its fundamentals and best practices for incident response. Includes the legal aspects of computer forensics, as well as its relationship to the Information Technology field. Hands-on projects will give students the tools and techniques to perform a full computer forensic investigation.

Prerequisite(s): TECH 223, IT 128, NSCOM 201, and NSCOM 227 or permission of the instructor.

Course Outcomes

- Discuss the fundamentals of computer forensics and its relationship with IT.
- Explain the legal aspects of computer forensics.
- Utilize best practices for incidence response.
- Analyze forensic data on multiple platforms Apply DOS, Windows and Linux tools for forensic analysis of seized media.
- Apply the necessary methodologies to conduct a computer forensic examination.
- Analyze network hardware involved in intrusion detection.
- Evaluate recovery tools and Network Attack Software.

ISIT 440 Administering a Linux Server – 5 credits

This course covers the essentials of Linux server administration. Students install, configure, use, secure and administer a Linux enterprise server. Topics include user access and security, process and service control, server monitoring, networks and networking services, interoperability, package management, backup and recovery and essential BASH commands.

Prerequisite(s): TECH 223 or permission of the instructor.

Course Outcomes

- Install, configure, use, secure and administer a Linux enterprise server.
- Manage user access and security.
- Manage and monitor processes and services.
- Harden the server by removing non-essential packages and files.
- Manage Linux using the BASH command line.
- Monitor and evaluate system integrity.
- Configure Linux for use a heterogeneous network environment.

ISIT 312 - Project Management for IT – 5 credits

Combines traditional project management with modern approaches adopted by lean and agile methods. Students will examine and apply project management concepts with emphasis on current IT methodologies and tools to gather information about the responsibilities and resources required to accomplish tasks and calculate the overall cost to plan a project. Students will define projects, determine resource requirements, write requests for proposals, define and sequence tasks, and create project schedules.

Prerequisite(s): Permission of instructor.

Course Outcomes

- Formulate problems and ideas or opportunities into clear objectives by defining project scope, choosing an approach and developing a project schedule and budget using both Predictive and Agile methodologies.
- Demonstrate proficiency in both writing and analysis of request-for-proposals.
- Develop and support processes to prioritize projects/initiatives, allocate resources, and track the performance of the project portfolio and related investments.
- Develop leadership, presentation and communication skills, formulate stakeholder management practices and apply team-building capabilities.
- Create deliverables, including a SWOT (strengths, weaknesses, opportunities, threats) analysis, program proposal, program charter and program objectives.
- Differentiate when PERT & GANT charts should be used and how to analyze them.
- Organize and design roles related to the Scrum framework including Development Team, Scrum Master and Product Owner.

ISIT 444 Automation/Configuration & Management – 5 credits

Introduces the concepts and application of basic scripting to monitor and collect logs in relation to servers and the associated services. Topics include scripting, logging, automation and system management.

Prerequisite(s): NSCOM 227, NSCOM 202, IT 128, and TECH 223 or permission of the instructor.

Course Outcomes

- Apply debugging techniques.

- Describe and apply scripting techniques for simple administrative tasks.
- Apply source code control systems for change management in various environments.
- Identify and apply best practices for system logging.
- Identify and apply best practices for system monitoring.
- Identify and apply best practices for system automation.
- Apply logging, monitoring and automation techniques in a homogenous environment.

ISIT 450 Network Vulnerabilities and Countermeasures – 5 credits

This course covers the concepts of network vulnerabilities from a hacker's perspective. Its focus is professional penetration testing and the securing of information assets. The course provides students with the knowledge to prevent, detect, and respond to network security incidents.

Prerequisite(s): TECH 223, NSCOM 202, and NSCOM 227 or permission of the instructor.

Course Outcomes

- Understand the importance of legal and ethical conduct in using computer network system.
- Effectively use appropriate information security software and assessment tools.
- Conduct security reconnaissance in order to identify network vulnerabilities and attack vectors.
- Evaluate where information networks are most vulnerable.
- Perform penetration tests into secure networks for evaluation purposes.
- Critique security plans designed at protecting data assets against attacks from the Internet.
- Develop an ongoing security strategy and investigate/mitigate data risk.
- Quantitatively assess and measure threats to information assets and implement proper safeguards based on risk analysis.

ISIT 452 Network Security Monitoring – 5 credits

This course focuses on the qualities that go into a sound Network Security Monitoring (NSM) system. Hands-on exercises use various network protocol analyzers and other tools to detect, investigate, and respond to network and system attacks. Students will learn how identify authorized and unauthorized malicious activity on an information systems network.

Prerequisite(s): NSCOM 202, TECH 223, and IT 128 or permission of the instructor.

Course Outcomes

- Explain fundamental concepts of Network Protocol Analysis.
- Assess the importance of ethical conduct when using computer networks.
- Collect, analyze, detect, and escalate unauthorized and authorized malicious network activity.
- Compare and contrast the skills needed to collect and analyze network packets using various open source tools.
- Install, configure, and use various network NSM and IDS (Intrusion Detection System) tools to collect, analyze, detect, investigate, escalate, and respond to network intrusions and attacks.
- Analyze the role of computer incident response team within organizations.

ISIT 454 System Hardening – 5 credits

Hardening a computer reduces the attack surface by disabling functionality that is not required while maintaining the minimum functionality that is required. Students will learn to apply the key system hardening principles of segregation of duties, dual control, principle of least privilege, and economy of mechanism. This course covers system hardening techniques for physical devices and connections, network devices, Windows and Unix/Linux server operating systems, and cross-platform applications.

Prerequisite(s): NSCOM 201, NSCOM 221, TECH 223, and IT 128 or permission of the instructor.

Course Outcomes

- Illustrate the necessity of planning as part of the system hardening process.
- Explain the rationale behind a hardening standard for systems such as physical devices and connections, network devices, Windows and Unix/Linux server operating systems and cross-platform applications.
- Implement a security standard for systems such as physical devices and connections, network devices, Windows and Unix/Linux server operating systems and cross-platform applications.
- Verify and evaluate the results of the system hardening process.

ISIT 490 ISIT Capstone I – 5 credits

This course provides practical experience in information systems and technology. Students apply knowledge and skills learned in classes as they work in settings relevant to their future employment plans. This is part 1 of a 2 quarter series.

Prerequisite(s): Permission of the instructor.

Course Outcomes

- Integrate skills and knowledge acquired from different courses and experiences.
- Develop and implement a project plan following appropriate methods and tools.
- Evaluate, develop and apply effective methods to manage project milestones and timelines.
- Demonstrate technical competency in completing deliverables.
- Work productively in a team environment communicating appropriately with all team members.
- Develop an effective report and presentation commensurate with the scope and complexity of the project.
- Present information in an effective format and discuss issues using a constructive approach.
- Demonstrate an in-depth and integrated understanding of the complexity of information technology and systems to peers and faculty

ISIT 491 ISIT Capstone II – 5 credits

Students continue their work from ISIT 490 to further develop their project work.

Prerequisite(s): ISIT 490 with a C or better.

Course Outcomes

- Integrate skills and knowledge acquired from Practicum I.
- Review, refine and adjust a work plan.
- Evaluate, develop and apply effective methods to manage project milestones and timelines.
- Demonstrate advanced technical competency in completing deliverables.
- Analyze task results, to include successes and areas for future improvement.
- Work productively in a team environment, if applicable to task, communicating professionally with all team members.
- Develop a professional report and presentation commensurate with the scope and complexity of the work.
- Present information in a professional format and discuss issues as the lead facilitator.
- Demonstrate an in-depth and integrated understanding of the complexity of information technology and systems to industry professionals.

Capstone 10 credits (see above) or EXPRL 490 and EXPL 491 Internship Experience 10 credits

Students document and reflect upon their internship experience to connect their learning to a real-world environment. Students will be advised by a faculty member and coached by an internship coordinator. Students must secure an approved internship before registering.

Prerequisite(s): Students admitted to applicable baccalaureate programs and with permission of instructors.

Course Outcomes

- Evaluate, integrate, and apply skills, concepts and knowledge acquired in the previous classes to real workplace situations and problems.
- Meaningfully synthesize connections between their internship work and their classroom studies in order to deepen their understanding of their program of study.
- Demonstrate technical competence to industry professionals by completing projects and deliverables assigned by their worksite supervisor.
- Identify and analyze strengths, new skills and knowledge acquired from the internship experience, interactions with colleagues and supervisors, and lessons learned in a reflective journal.
- Document internship accomplishments and activities and articulate the value of those activities and accomplishments.
- Create a strengths-based LinkedIn profile and resume in preparation for full-time employment after graduation.
- Select a career goal and articulate how their BC education has prepared them for that goal and how they plan to continue their learning after graduation.

BUS 355 Business of IT: Legal Regulatory Business Environment – 5 credits

This course focuses on managerial and legal principles and knowledge that are critical to IT organizations and the management of organizations focused on information technology in the modern business world. Students will develop skills and techniques in the areas of the relevant legal concepts and doctrines; regulatory and administrative agency requirements; and organizational development and management practice applicable in the IT environment. Case studies will be used.

Prerequisite(s): BUS 101.

Course Outcomes

- Evaluate the legal and ethical standards IT professionals and managers must maintain.
- Explain the legal and regulatory powers and structures of administrative agencies and devise strategies to optimize business interactions with them.
- Illustrate appropriate approaches for meeting the requirements for legal compliance within regulatory agencies including analyzing and describing HIPAA, NIST, LEED, SOX, and other finance and accounting legal standards as they apply to the IT environment.
- Analyze and evaluate the legal and ethical dimensions of contracts and legal devices and doctrines applicable to the IT environment including intellectual property rights, employment contracts, nondisclosure agreements, vendor contracts, agency, employment, and independent contractor law.
- Interpret the relationship between ethical values and legal requirements.
- Appraise contemporary practices, challenges, and opportunities at the intersection of IT and corporate governance.
- Appraise contemporary management practices and organizational behavior theory particularly applicable to the IT environment and IT organizations including change management.
- Explain and demonstrate good business judgment in making IT decisions based on economic analysis, including TCO (Total Cost of Ownership), ROI, (Return on Investment), and lease versus buy considerations.
- Discriminate, evaluate, and apply management theories and principles in the IT environment such that IT systems and organizations remain in compliance including the requirement of a formal, controlled change management system.

CMST 340 Advanced Communication in Business & Technology – 5 credits

This course is designed for students accepted into a baccalaureate degree program in business or technology fields. Students identify, self-assess, analyze and apply skills to effectively communicate in culturally diverse business and technology settings. Students explore original research and apply the information they learn to their communication skill repertoire. Topics include: active listening, intercultural communication, collaborating in teams, conflict management, verbal and nonverbal communication and public speaking.

Recommended: CMST 220, CMST 230, or CMST 280.
Prerequisite(s): Acceptance into applicable baccalaureate program or permission of instructor.

Course Outcomes

- Self-assess one's own communication behaviors and effects.

- Explain and demonstrate active listening and communication competence.
- Evaluate the types of language and nonverbal communication that promote effective communication within the business and technology fields.
- Explain which communication behaviors promote effective teamwork, collaboration and decision-making in a diverse group setting.
- Self-assess one's own biases and practice intercultural competence in the business and technology settings.
- Evaluate and practice appropriate approaches for effective conflict management in a variety of settings.
- Develop and deliver presentations that apply elements of effective public speaking to a variety of audiences and situations.

PHIL& 115 Critical Thinking – 5 credits

An informal, non-symbolic introduction to logic and critical thinking emphasizing real-life examples, natural language applications, and the informal logical fallacies.

Course Outcomes

- Formulate, clarify and evaluate arguments.
- Explain and use basic philosophic concepts relevant to critical thinking (e.g., truth, validity, soundness, strength, cogency).
- Recognize and name informal fallacies.
- Analyze and evaluate arguments in scientific, causal and analogical reasoning.
- Analyze and evaluate developed arguments in context.

PHIL 375 Ethical Issues in Information Technology – 5 credits

Investigates ethical problems relating to information technology through ethical theory and case studies. Involves in-depth and original research and discussion of ethical issues including privacy, control of information and intellectual property rights. Designed for students in four-year Information Technology degree programs at Bellevue College.

Prerequisite(s): Acceptance to the program or permission of the instructor.

Course Outcomes

- Explain and evaluate ethical principles and the philosophical arguments that bear on them.
- Apply ethical principles to a broad range of issues in information technology including intellectual property rights, privacy, freedom of expression and information security.
- Recognize and develop strategies for dealing with varying cultural perspectives on IT related ethical issues.
- Apply ethical principles in detailed case studies.
- Evaluate arguments for and against proposed solutions to ethical dilemmas in information technology.

Appendix C: External Expert Review

INSTRUCTIONS FOR COLLEGES SUBMITTING A BAS DEGREE PROPOSAL:

1. As part of completing a program proposal, colleges must select two external experts to review the program.
2. Reviews should be completed by an independent, third-party person or team with subject/discipline expertise.
3. At least one, preferably two, of these external expert reviewers should come from a university level institution, i.e. departmental professor, academic dean or department head.
4. A second external expert reviewer may be a professional/practitioner who works for a private or public organization other than the university.
5. External Expert Reviewers should be instructed by colleges to address the criteria listed in this rubric.

INSTRUCTIONS FOR EXTERNAL EXPERT REVIEWERS:

1. External Expert Reviews provide critical feedback to colleges so that they may address potential concerns, issues or criticisms prior to final submission of a program proposal to the State Board of Community and Technical Colleges.
2. Reviewers should be independent, third-party persons or teams with subject/discipline expertise.
3. The goal of a review is to assess the credibility, design, relevance, rigor, and effectiveness of the proposed BAS program.
4. Reviewers should also validate the congruency and consistency of the program's curriculum with current research, academic thinking and industry standards.
5. Reviewers need not provide responses to every criteria listed in the Rubric. If reviewers feel that they cannot adequately address any one of the criteria, they may simply state that this is the case.
6. This form is designed to assist External Expert Reviewers to complete assessments of baccalaureate degree program proposals. External Expert Reviewers are not restricted to the use of this rubric template. Reviewers may choose, instead, to provide a college with a written narrative. In whatever format they choose, reviewers should address the criteria outline in the rubric.

Applied Baccalaureate External Review Rubric

College Name:	Belleve College	**BAS Degree Title:**	Bachelor of Applied Science in Cybersecurity
Reviewer Name/ Team Name:	Professor Yan Bai	**Institutional or Professional Affiliation:**	University of Washington Tacoma
Professional License or Qualification, if any:	Ph.D.	**Relationship to Program, if any:**	N/A

Please evaluate the following Specific Elements	
a) Concept and overview	Is the overall concept of the degree program relevant and appropriate to current employer demands as well as to accepted academic standards? Will the program lead to job placement?
	Comment **The Bachelor of Applied Science in Cybersecurity at Belleve College will address the needs of cybersecurity workforce development. The curriculum and technical courses cover important domains of cybersecurity.**
b) Degree Learning Outcomes	Do the degree learning outcomes demonstrate appropriate baccalaureate degree rigor?
	Comment **The program outcomes are well designed, and will be assessed from various pespectives of different stakeholders. However, it would be better to add some detailed info for mapping different BAS in Cybersecurity courses to program learning outcomes.**
c) Curriculum Alignment	Does the curriculum align with the program's Statement of Needs Document?
	Comment

	The curriculum targets the need for a cybersecurity workforce. But, the needs for Bachelor’s degree are not very clearly stated. I suggest adding info about the need for a cybersecurity workforce with Bachelor’s degree. Perhaps a survey of alnumni of BAS IST with concentration in Cyber Security and Systems can help.
d) Academic Relevance and Rigor	Do the core and elective courses align with employer needs and demands? Are the upper level courses, in particular, relevant to industry? Do the upper level courses demonstrate standard academic rigor for baccalaureate degrees?
	Comment **‘Yes’ to all of the 3 questions, and I have no additional comments.**
e) General Education Requirements	Are the general educations requirements suitable for a baccalaureate level program? Do the general education courses meet breadth and depth requirements?
	Comment **‘Yes’ to all of the 2 questions; I have no additional comments.**
f) Preparation for Graduate Program Acceptance	Do the degree concept, learning outcomes and curriculum prepare graduates to enter and undertake suitable graduate degree programs?
	Comment **The technical courses are good for students who have successfully completed BAS in Cybersecurity at Bellevue College to pursue advanced study. However, information stated in the section about Criteria 7 on Page 20 of the degree proposal is not appropriate.**

	“While all BAS graduates can apply to any Master’s degree program, institutions who have discussed the graduate pathway with Bellevue College for the Bachelor of Applied Science Cybersecurity include: • …. • UW Tacoma: Master’s in Cybersecurity and Leadership These programs have already identified that the BAS Cybersecurity curriculum will meet their enrollment expectations for their Master’s level programs. ” **As the Director of Master of Cybersecurity & Leadership (MCL) program, I am aware that we have NOT discussed with Bellevue College about any pathway between UW Tacoma MCL and the proposed BAS in Cybersecurity at Bellevue College. We have not identified that the BAS in Cybersecurity curriculum at Bellevue college will meet enrollment expectations for our MCL program.**
g) Faculty	Do program faculty qualifications appear adequate to teach and continuously improve the curriculum?
	Comment **Some of exisiting faculty members have expertises in Cybersecurity and Information Techology. They might not be able to cover all of the courses in BAS. The new faculty with different expertises is helpful.**
h) Resources	Does the college demonstrate adequate resources to sustain and advance the program, including those necessary to support student and library services as well as facilities?
	Comment **The college has extensive resources to support student success as described in Criteria 4.**

i) Membership and Advisory Committee	Has the program received approval from an Advisory Committee? Has the program responded appropriately to it Advisory Committee's recommendations?
	Comment **The proposal does not include the information about the discussion of and approval from an Advisory Committee about the BAS in Cybersecurity degree proposal.**
j) Overall assessment and recommendations	Please summarize your overall assessment of the program.
	Comment **The program is well designed to provide students with technical knowledge in Cybersecurity, and will address cyber workforce needs. The proposal has good program evalulation criteria for different stakeholders.** **Some statements are not accurate in the section on Criteria 7 on Page 20 of the degree proposal. They should be corrected.**
Reviewer Bio or Resume Evaluator, please insert a short bio here Yan Bai is the Director of Master of Cybersecurity & Leadership Program, and a Professor in the School of Engineering and Technology, University of Washington Tacoma, USA. Dr. Bai received her Ph.D. in Electrical and Computer Engineering from the University of British Columbia, Vancouver, BC, Canada. She has taught undergraduate and graduate courses in computer networks, computer security, network security, information assurance and digital forensics and supervised more than 200 students in research projects and internships.	

She has published over 80 refereed papers in computer networking and cybersecurity areas. She has served as a General Chair/Program Chair/Technical Program Committee Member for numerous IEEE conferences and workshops, and as a Reviewer for a wide range of high impact research journals and ACM/IEEE flagship conferences.

Applied Baccalaureate External Review Rubric

College Name:	Bellevue College	**BAS Degree Title:**	BAS Cybersecurity
Reviewer Name/ Team Name:	Erik Fretheim	**Institutional or Professional Affiliation:**	Western Washington University
Professional License or Qualification, if any:		**Relationship to Program, if any:**	
Please evaluate the following Specific Elements			
a) Concept and overview	Is the overall concept of the degree program relevant and appropriate to current employer demands as well as to accepted academic standards? Will the program lead to job placement?		
	Comment **Overall concept is relevant and needed. There are three listed areas of competency in the program description – monitor and maintain, translate policy to technical architecture, and system administration. Recommend the program review the NIST/NICE job roles (https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework), determine which are the most relevant for program graduates and map the knowledge, skills, and abilities for those. This will help to identify gaps, and areas which may not be needed.**		
b) Degree Learning Outcomes	Do the degree learning outcomes demonstrate appropriate baccalaureate degree rigor?		
	Comment **There are 10 outcomes. That is a lot. The first one, is rather vague and as the concepts are in the others, it could be eliminated without any loss. The last outcome is not an outcome, but a program requirement. Possibly the local and global impact outcome could be combined with sustainable business practices to further reduce to a more manageable 7.**		
c) Curriculum Alignment	Does the curriculum align with the program's Statement of Needs Document?		
	Comment		

	See recommendation for NIST/NICE in a) above.
d) Academic Relevance and Rigor	Do the core and elective courses align with employer needs and demands? Are the upper level courses, in particular, relevant to industry? Do the upper level courses demonstrate standard academic rigor for baccalaureate degrees?
	Comment **5 Credits per course for every course appears a bit high. It doesn't leave much flexibility within the programs, and the outcomes in the classes don't support the high level of credits. 5 credits per quarter would represent 150 hours (50 in class, 100 out of class) of study of a topic in a quarter. For some courses as described, this would be a matter of squeezing 30 hours of class into 50. Adjusting the credits of the courses would also allow for a more rounded degree through the inclusion of open electives.** **Courses have outcomes based on, and appear to be built around, specific technologies rather than addressing core concepts and using specific technologies to illustrate them. As technologies change, this will be an issue as the skills and knowledge will not translate to new technologies.** **There is no programming in the program and scripting is only one of seven course outcomes in a single course. Cyber professionals can be expected to apply significant amounts of programming and scripting skills in the course of their duties. This is an essential skill at all levels.** **Risk management is not addressed in the program.** **Really good that the program includes Project Management. That was a good choice.** **I did not see specifics of the outcome:** Identify and analyze user needs and take them into account in the selection, creation, evaluation, implementation and administration of technology systems; **addressed in the courses.** **Digital Forensics is an odd inclusion on a list of courses which doesn't fall under any of the three areas of focus listed in the program description, nor under any of the outcomes. Forensics is a specific subfield which graduates would be unlikely to encounter, or if they did, would not be prepared from a single course. It**

	is a popular course, similar to penetration testing/red teaming. However, neither are sufficiently addressed in a single course and students would be unlikely to find employment in the area based on a single course. I am confused as to the purpose of ISIT 454 System Hardening. It would appear that the topics are addressed in previous courses.— Under program specific accreditation, only NWCCU is listed with a mention of assessing potential benefits of program specific accreditation. In the field of cybersecurity, the gold standard is the NSA/DHS CAE program (https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/). Even if a program decides not to pursue this route, it should consider it as a part of its program development. In addition, ABET offers program accreditation for Cybersecurity programs (https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2021-2022/). Again, while there is not a need for immediate pursuit of a program specific accreditation, the positioning of the program relative to such accreditation should be considered.
e) General Education Requirements	Are the general educations requirements suitable for a baccalaureate level program? Do the general education courses meet breadth and depth requirements?
	Comment Although the technical numbers are met, there isn't much flexibility for students, and it looks like the program tries to meet the requirements without stepping very far from the program focus. Part of the purpose of the General Education Requirements is to broaden the students' perspectives.
f) Preparation for Graduate Program Acceptance	Do the degree concept, learning outcomes and curriculum prepare graduates to enter and undertake suitable graduate degree programs?
	Comment If the students are interested in pursuing a management focused graduate program, they would appear to have a fairly good background. If they are interested in a technically focused graduate program, they will have significant theoretical shortfalls.

g) Faculty	Do program faculty qualifications appear adequate to teach and continuously improve the curriculum?
	Comment **While the faculty appear to have industry experience, they are significantly lacking in academic qualifications. There are no full-time faculty with a relevant master's degree, and only 1 with a relevant BS. Part-time faculty are also lacking relevant degrees. While the faculty are undoubtedly experienced and provide some quality instruction, the lack of experience in academic areas is a cause for concern. Not all faculty need higher degrees, but at least some should have one.**
h) Resources	Does the college demonstrate adequate resources to sustain and advance the program, including those necessary to support student and library services as well as facilities?
	Comment Yes.
i) Membership and Advisory Committee	Has the program received approval from an Advisory Committee? Has the program responded appropriately to it Advisory Committee's recommendations?
	Comment N/A
j) Overall assessment and recommendations	Please summarize your overall assessment of the program.
	Comment The program as described has the beginnings of a good program. There should be more work in focusing on the objectives of the program and comparing the proposed content with established criteria, such as NICE

<table>
<tr><td></td><td>NIST, NSA/DHS CAE, and others. This not only helps the program establish its content, but also gives potential students assurance that their education is generally applicable and meets industry needs.</td></tr>
<tr><td colspan="2"><b>Reviewer Bio or Resume</b>
Evaluator, please insert a short bio here

Dr. Fretheim is the Cybersecurity Programs Director at Western Washington University.   Prior to joining WWU, Dr. Fretheim was a Professor and Executive Director of the Technology Institute at City University of Seattle, and a Professor at the United States Military Academy, at West Point, NY. Colonel Fretheim retired from the US Army Reserves after 33 years of active and reserve service, where he was a Signal Officer. His awards include the Bronze Star, Meritorious Service Medal with Oak Leaf Cluster, and various other awards and service ribbons. In addition to his time in the Army, Dr. Fretheim spent time in Senior Engineering, and Executive Management at a number of companies including MCI, Siemens Business Services, i5Digital, and other telecom and technology companies, as well as being a consultant in Cybersecurity and Engineering Leadership.   Dr. Fretheim has a BS in Electrical Engineering and Computer Science from the US Military Academy, an MSEE and PhD from the Air Force Institute of Technology, and an MBA from Long Island University. He is a Senior Member of the IEEE, a Director of the Colloquium on Information Systems Security Education, and sits on the board of several non-profits.</td></tr>
</table>