SAINT LOUIS UNIVERSITY.

Program-Level Assessment: Annual Report

Program Name (no acronyms): Cybersecurity	Department: SPS Graduate Programs
Degree or Certificate Level: Master's of Science	College/School: Professional Studies
Date (Month/Year): August/2022	Primary Assessment Contact: Maria Weber

In what year was the data upon which this report is based collected? 2022

In what year was the program's assessment plan most recently reviewed/updated? 2022

1. Student Learning Outcomes

Which of the program's student learning outcomes were assessed in this annual assessment cycle? (Please list the actual learning outcome statements and not just numbers, e.g., Outcomes 1 and 2.)

SLO 1: Graduates will be able to apply program-specific knowledge to address practical problems using an ethical, evidence-based framework

SLO 2: Graduates will be able to utilize argumentation skills appropriate for a given problem or context.

2. Assessment Methods: Artifacts of Student Learning

Which artifacts of student learning were used to determine if students achieved the outcome(s)? Please identify the course(s) in which these artifacts were collected. Clarify if any such courses were offered a) online, b) at the Madrid campus, or c) at any other off-campus location.

Our new assessment protocol integrates data from three sources to evaluate student learning:
1. Each program LO is mapped to specific courses and artifacts within those courses (see below). Instructors complete an assessment of learning that is attached to the rubric of the artifact's grading rubric. It is important to note that this process is meant to gather data that is independent of grades given.
2. Faculty mentors complete a summative assessment on each student at the conclusion of their capstone. Mentor's assess the student's performance for each of the learning outcomes.
3. A student assessment of learning outcomes is also completed by students at the end of their degree. This indirect measure asks students to rate the extent they learned and developed on each LO. They also indicate what specific competencies they developed and which they feel they need additional development.

Data from individual students and students completing the master's research project (CYBR 5963)
SLO 1: Graduates will be able to apply program-specific knowledge to address practical problems using an ethical, evidence-based framework.

CYBR 5000, Cybersecurity Principles
<u>Fall 2021</u>
CYBR-5000 -11 - 12 students * Final Project

CYBR 5210, Digital Investigations
No offered

CYBR 5230, Intrusion Detection and Analysis
No Offered

CYBR 5961/ CYBR 5262/ CYBR 5963 -Master Research Project I/II/III
Summer 2021
CYBR-5961 -11 - 1 students * - Master Research Prospectus
CYBR-5961 -21 - 1 students * - Master Research Prospectus
Fall 2021
CYBR-5962 -21 - 2 students * Master Research Proposal
CYBR-5963-21 - 4 students* Master Research Project
Spring 2022
CYBR-5963 -21 - 3 students * Master Research Project

SLO 2: Graduates will be able to utilize argumentation skills appropriate for a given problem or context.

CYBR 5000, Cybersecurity Principles
Fall 2021
CYBR-5000 -11 - 12 students * Final Project

CYBR 5220, Incident Response and Mitigation
Fall 2021
CYBR-5220 -21 - 4 students * Final Project

CYBR 5240, Cloud Security
Summer 2021
CYBR-5240- 11 - 8 students * Final Project
Spring 2022
CYBR-5240 -11 - 5 students * Final Project

CYBR 5961/ CYBR 5262/ CYBR 5963 -Master Research Project I/II/III
Summer 2021
CYBR-5961 -11 - 1 students * - Master Research Prospectus
CYBR-5961 -21 - 1 students * - Master Research Prospectus
Fall 2021
CYBR-5962 -21 - 2 students * Master Research Proposal
CYBR-5963-21 - 4 students* Master Research Project
Spring 2022
CYBR-5963 -21 - 3 students * Master Research Project

Legend: * Courses were taught 100% online
**Courses were taught 100% on-campus
Note: No courses offered in Madrid Campus

3. Assessment Methods: Evaluation Process

What process was used to evaluate the artifacts of student learning, and by whom? Please identify the tools(s) (e.g., a rubric) used in the process and include them in/with this report.

The artifacts were evaluated by the program director in consultation with the course instructor. The evaluation involved one instructor for each course (i.e., one for CYBR 5000, another for CYBR 5010, etc.) Each artifact is assessed according to a standard rubric in Canvas. Within Canvas we then attach associated learning outcome measures to those rubrics. Instructors, after grading the artifact, rate the student in terms of their learning mastery. The learning outcome assessment is separate from the grade given on the assignment. We pulled raw survey data from each of the courses in Canvas. We then tabulated the quantitative data to provide a high-level overview. Please note that the Canvas approach was new this year. Previously, data was collected independently through a survey in Qualtrics

4. Data/Results

What were the results of the assessment of the learning outcome(s)? Please be specific. Does achievement differ by teaching modality (e.g., online vs. face-to-face) or on-ground location (e.g., STL campus, Madrid campus, other off-campus site)?

The Canvas outcomes reported that many of the artifacts had properly assessed student learning outcomes for their specific courses, but some minor adjustments might be needed; which will be explained further in section 5 of this report. Most instructors used final projects as their assessment tool and felt it was appropriate for the type of students in these classes.

SLO 1: Graduates will be able to apply program-specific knowledge to address practical problems using an ethical, evidence-based framework.

The majority of students were thoroughly introduced to SLO 1 in CYBR-5000 100% in Fall 1 2022, which is the first course for the master of Cybersecurity. All courses were offered online.

CYBR 5000, Cybersecurity Principles

Fall 2021

CYBR-5000 -11 - 12 students * Final Project 75% Meet Standard - 25% Approaches StandardCritical Security Controls White Paper. Each student will write a white paper based on the CIS Top 20 Security Controls found in Canvas. Studentsare given the task to act as an external consultant to advise a hypothetical CIO/CISO.. Consultants should prioritize 3-5 Top 20 controls (based on risk the company has) that the CIO/CISO should implement. Additionally, students should record a 5-10 minute executive summary presentation to the CIO/CISO * - - 75% Meet Standard and were able to successfully choose and prioritize 3-5 Top 20 controls, and communicate the findings in a recorded video. the CIS Top 20 Security Controls-These students were able to apply the Cybersecurity concepts learned in this course to address this case scenario. They also used evidence-based to support their choices and communicate it clearly. 25% Approaches Standard because even though students were able to successfully prioritize the critical controls, they did not use in-text citation or references to justify their writing proposal or within the presentation.

CYBR 5961/ CYBR 5262/ CYBR 5963 -Master Research Project I/II/III

Summer 2021

CYBR-5961 -11 - 1 students * - Master Research Prospectus - 100% Meet Standard All students identified the purpose and scope of the problem they intend to address. Students wearable to use evidence-based in the prospectus by choosing 10 articles and white paper that support their project/ Students choose 10 articles (peer-review, journal, white-papers to justify their findings)

CYBR-5961 -21 - 1 students * - Master Research Prospectus - 100% Meet Standard All students identified the purpose and scope of the problem they intend to address.Students wearable to use evidence-based in the prospectus by choosing 10 articles and white paper that support their project. Students choose 10 articles (peer-review, journal, white-papers to justify their findings)

Fall 2021

CYBR-5962 -21 - 2 students * Master Research Proposal - 100% Meet Standard - students created an applied research design that includes a proposal for addressing the organizational problem that was identified and described in CYBR 5961. Students choose an additional 10 articles (peer-review, journal, white-papers to justify their findings) All the argumentation and rebuttal is based on evidence that student provided.

CYBR-5963-21 - 4 students* Master Research Project - 100% Meet Standard - students implemented an applied research project to address an organizational or societal problem, written a formal report of findings and recommendations, and produced a reflection of their experiences and its implications for their future. In the case of a prototype-based project, the student implemented the prototype to meet the specifications determined in the previous two courses in the sequence.Students successfully utilized the evidence-based framework to develop their project, write their papers, create their prototypes and communicate it to the faculty/mentor(s)

Spring 2022

CYBR-5963 -21 - 3 students * Master Research Project - 100% Meet Standard - students implemented an applied research project to address an organizational or societal problem, written a formal report of findings and recommendations, and produced a reflection of their experiences and its implications for their future. In the case of a prototype-based project, the student implemented the prototype to meet the specifications determined in the previous two courses in the sequence. .Students successfully utilized the evidence-based framework to develop their project, write their papers, create their prototypes and communicate it to the faculty/mentor(s)

SLO 2: Graduates will be able to utilize argumentation skills appropriate for a given problem or context.
CYBR 5000, Cybersecurity Principles
Fall 2021
CYBR-5000 -11 - 12 students * Final Project 75% Meet Standard - 25% Approaches Standard Critical Security Controls White Paper. Each student will write a white paper based on the CIS Top 20 Security Controls found in Canvas. Studentsare given the task to act as an external consultant to advise a hypothetical CIO/CISO.. Consultants should prioritize 3-5 Top 20 controls (based on risk the company has) that the CIO/CISO should implement. Additionally, students should record a 5-10 minute executive summary presentation to the CIO/CISO * - - 75% Meet Standard and were able to use argumentation skills appropriate to the proposed problem: 3-5 Top 20 controls, and communicate the findings in a recorded video. the CIS Top 20 Security Controls- 25% Approaches Standard because they did not use appropriate argumentation skills within their projects.

CYBR 5220, Incident Response and Mitigation
Fall 2021
CYBR-5220 -21 - 4 students * Final Project 75% Meet Standard - 25% Approaches Standard. - Students are working on the blue team for a financial services organization (e.g. Edward Jones, etc.). You are being asked to prepare a report for the CIO/CISO on an on-going security incident that is being executed against your company from an Eastern European based hacking group.
75% of the students meet the requirement using argumentation skills to build up the incident report. Explain the rationality for all the steps taken and the possible resolution

CYBR 5240, Cloud Security
Summer 2021
CYBR-5240- 11 - 8 students * Final Project - 100% Meet Standard Students worked individually to demonstrate their knowledge of Cloud Security by applying the concepts and theories to create a Final Paper. Students sucessfully Described the processes and reference NIST Frameworks to ensure Cloud Computing Security efforts capitalize on lasting security value to the institution. Students used argumentation skills when comparing three major CSPs suh as GCP, AWS, and Azure

Spring 2022
CYBR-5240 -11 - 5 students * Final Project - 100% Meet Standard Students worked individually to demonstrate their knowledge of Cloud Security by applying the concepts and theories to create a Final Paper. Students sucessfully Described the processes and reference NIST Frameworks to ensure Cloud Computing Security efforts capitalize on lasting security value to the institution.Students used argumentation skills when comparing three major CSPs suh as GCP, AWS, and Azure

CYBR 5961/ CYBR 5262/ CYBR 5963 -Master Research Project I/II/III
Summer 2021
CYBR-5961 -11 - 1 students * - Master Research Prospectus - 100% Meet Standard All students identified the purpose and scope of the problem they intend to address.Students were able to use evidence-based in the prospectus by choosing 10 articles and white paper that support their project. These articles are used in in-text citations and references to defend, probe or disprove a theory or a hypothesis.
CYBR-5961 -21 - 1 students * - Master Research Prospectus- 100% Meet Standard All students identified the purpose and scope of the problem they intend to address.Students wearable to use evidence-based in the prospectus by choosing 10 articles and white paper that support their project. These articles are used in in-text citations and references to defend, probe or disprove a theory or a hypothesis.
Fall 2021
CYBR-5962 -21 - 2 students * Master Research Proposal - 100% Meet Standard - Students created an applied research design that includes a proposal for addressing the organizational problem that was identified and described in CYBR 5961. Students choose an additional 10 articles (peer-review, journal, white-papers to justify their findings) All the argumentation and rebuttal is based on evidence that student provided.
CYBR-5963-21 - 4 students* Master Research Project - 100% Meet Standard students implemented an applied research project to address an organizational or societal problem, wrote a formal report of findings and recommendations, and

produced a reflection of their experiences and its implications for their future. In the case of a prototype-based project, the student implemented the prototype to meet the specifications determined in the previous two courses in the sequence..Students successfully utilized the argumentation skills to compare and contrast their project, write their papers, create their prototypes and communicate it to the faculty/mentor(s)

Spring 2022

CYBR-5963 -21 - 3 students * Master Research Project - 90% Meet Standard and 10 % Approaches Standard - students implemented an applied research project to address an organizational or societal problem, written a formal report of findings and recommendations, and produced a reflection of their experiences and its implications for their future. In the case of a prototype-based project, the student implemented the prototype to meet the specifications determined in the previous two courses in the sequence. .Students successfully utilized the argumentation skills to compare and contrast their project, write their papers, create their prototypes and communicate it to the faculty/mentor(s)

Attached is the Learning Outcome Rubric which is used by the faculty to assess the SLOs

5. Findings: Interpretations & Conclusions

What have you learned from these results? What does the data tell you?

General Conclusions: Most of the students that approached the standard because they stopped participating in the class (and thus did not submit the final assignment/artifact) or they did not submit the final assignment/artifact after completing other assignments in the course or they did not submit an assignment/artifact that fulfill the criteria to meet the standard. To put this in perspective, a total of 3 students across CYBR-5000, CYBR-5961, CYBR-5962, and CYBR-5963 approached the standard for SLO 1. Of these 3 students, 1 of them failed to approach the standard because they did not submit the assignment/artifact and 2 of them did not submit an assignment/artifact that fulfilled the criteria to meet the standard. This means, then, that 13 % did not approach the standard while 87% met the standard, and 0% did not meet the standards. A total of 4 students across CYBR-5000, CYBR-5220, CYBR-5240, CYBR-5961, CYBR-5962, and CYBR-5963 did not approach the standard for SLO 2. Of these 4 students, 2 failed to meet the standard because they did not submit the assignment/artifact and 2 did not submit an assignment/artifact that fulfilled the criteria to meet the standard. This means, then, that 10% did not approach the standard, while 0% did not meet the standard, and 90% met the standard. We need to understand why a fair number of students are not fulfilling the criteria for the assignments or submitting the final assignments/artifacts. It is not uncommon when teaching adult students with work and family responsibilities. However, it could be the case that some students are “intimidated” by the final assignment. Do we need to provide sufficient and more explicit instructions for the assignments? Do students feel comfortable with the instructions? While I think it is good that 87% of students approached or met the standard for SLO 1, 90% approached or met the standard for SLO 2, I think more needs to be done to increase the percentage of students that meet the standard for each SLO.

SLO 1:

In the Summer 1 and 2 of 2021 section of CYBR 5961 (Master Research Project I), 100% of the students met the standard. In the Fall 2021 section of CYBR 5961 (Master Research Project , 100% of the students met the standard.The entire cohort of CYBR-5961 were adult students who were already working. They were able to get permission to address company issues in their master research projects. Students were able to use the knowledge based learned in the master program in proposing solutions for their company issues with the evidence-based approach. Projects type included: phishing, agent-based remediation, cloud computing, among other topics.In the Fall 1 2021 section of CYBR-5000 (Cybersecurity Principles), 0% of the students did not meet the standard, 25% approached the standard, and 75% met the standard. This is the first course of the degree and 25% students struggled with time-management skills to meet the deadlines during the first week. While the student population is purely working adults, assignments need to be shifted and distributed so the first week of class students can adapt well to the course.In the Fall 2 2021 section of CYBR 5962 (Master Research Project II) and CYBR 5963 (Master Research Project III), 100% of the students met the standard. The master research project is a 3-course sequence. Once the students choose a project in Master Research Project I, they need to develop a proposal, prototype, write a paper, and present. Students were comfortable with their soft skills since they are already working, they have good communication skills. Master Research Projects were so well done that the students obtained jobs, got promotions, or recognition from their company mentors. A student in particular used an evidence-based framework to compare how much time, cost, and labor were involved on a manual vs. surgical remediation. This student developed a Monte Carlo Simulation model to analyze the data.

In summary, a total of 23 students enrolled in Cybersecurity courses, 20 (87%) students meet standard, 3 (13%) students have Approaches Standard, and 0% Do not meet standard. During the 2021-22 Academic Year 87 % of the students meet the standard of SLO1.

SLO2

In the Summer 1 of 2021 section of CYBR 5240 (Cloud Security) 100% of the students met the standard. Students were able to use argumentation skills in the weekly case studies. In Summer 1 and 2 of the 2021 section of CYBR 5961 (Master Research Project I), 100% of the students met the standard. These students used company-based project also since they are working in the field of Cybersecurity and with the knowledge acquire in the masters were able to met the standard..In the Fall 1 2021 section of CYBR-5000 (Cybersecurity Principles), 0% of the students did not meet the standard, 25% approached the standard, and 75% met the standard. Students who did not approach the standard did not meet the criteria for assignments where they needed to demonstrate argumentation skills to justify their findings in the final project. In the Fall 1 2021 section of CYBR-5220 (Incident Response and Mitigation), 0% of the students did not meet the standard, 25% approached the standard, and 75% met the standard. Students who did meet the standard did not complete the assignments/artifacts. This course has several hands-on activities, those were achieved by all the students. Issues were seen in the discussion boards. Students will need additional instruction in how to develop a good discussion prompt, reply to peers, and defend/refute their position. Students did well in their final project. In the Fall 2 2021 section of CYBR 5962 (Master Research Project II) 100% of the students met the standard. Students in this course had already developed a prospectus and built up the proposal using argumentation skills based on the evidence they collected. In Spring 2 2022, a section CYBR 5963 (Master Research Project III), 100% of the students met the standard. Students completed their Master Research Project written paper and presentation.Student used argumentation skills to present/defend their findings and recommendations. In Spring 1 2022, a section CYBR 5240 (Cloud Security) 100% of the students met the standard. As in the summer, students continue performing very well in this course. The approach in the course is for the students to work on GCP, AWS, and Azure to be able to properly compare and contrast in the final project each of these cloud providers and use argumentation skills with the evidence learned in hands-on activities in each of these providers.

In summary, a total of 40 students enrolled in Cybersecurity courses, 36 (90%) students Meet Standard, 4 (10%) students Approach the Standard, 0% Do not meet standard. During the 2021-22 Academic Year 90 % of the students meet the standard of SLO2.

6. Closing the Loop: Dissemination and Use of Current Assessment Findings

A. When and how did your program faculty share and discuss these results and findings from this cycle of assessment?

The program director and faculty met at the end of Spring 2022 to discuss the results. We went through the data and discussed variables that might have impacted the data. We also discussed potential changes whether pedagogical or curricular. We discussed whether we needed a different artifact (e.g., an essay instead of an exam), whether we needed to change the expectations in our assignment prompts, or whether we needed to change our teaching techniques.

B. How specifically have you decided to use these findings to improve teaching and learning in your program? For example, perhaps you’ve initiated one or more of the following:

Changes to the Curriculum or Pedagogies	● Course content ● Teaching techniques ● Improvements in technology ● Prerequisites	● Course sequence ● New courses ● Deletion of courses ● Changes in frequency or scheduling of course offerings
Changes to the Assessment Plan	● Student learning outcomes ● Artifacts of student learning ● Evaluation process	● Evaluation tools (e.g., rubrics) ● Data collection methods ● Frequency of data collection

Please describe the actions you are taking as a result of these findings.

No changes to the assessment plan at this point. Based on student and faculty feedback, course frequency and scheduling are being revised to level the number of courses offered each term. We will refine our assignment prompts: more emphasis on applying evidence-based framework (SLO 1) in CYBR-5000 and more emphasis on argumentation skills (SLO 2) in CYBR-5220. We will also change our discussion techniques in CYBR-5220 and CYBR-5000. More clear instructions in the assignment/artifact to encourage students to integrate evidence-based, argumentation skills and experiences. We feel that students need more instruction on this mode of writing. We will add material to the courses CYBR–5000 and CYBR-5220 (writing resources and sample deliverables for labs/hands-on activities).

If no changes are being made, please explain why.

7. Closing the Loop: Review of Previous Assessment Findings and Changes

A. What is at least one change your program has implemented in recent years as a result of assessment data?

Previous year we worked on standardization of the Master Research Project options with their respective templates. The hiring of new adjuncts and redesigning courses has begun according to the revised curriculum map.

B. How has this change/have these changes been assessed?

The Master Research projects have been evaluated by faculty mentors who work with students throughout the three-hour sequence. Students implemented an applied research project consistent with their approved project, wrote a formal report of findings and recommendations, and delivered a formal presentation summarizing the project. 100% Students in Master Research Project I,II, and III met the standard. This shows how the changes done in the previous year were successfully implemented.

C. What were the findings of the assessment?

Students who completed the three-hour sequence satisfactorily demonstrated the competencies gained during the MS Cybersecurity program.100% met the standard

D. How do you plan to (continue to) use this information moving forward?

The four general Master Research Project options will continue to be offered to students. Courses CYBR-5000 and CYBR-5220 will have some redesign.

IMPORTANT: Please submit any assessment tools (e.g., rubrics) with this report.

Cybersecurity
Learning Outcomes Rubric

Learning Outcome	Does Not Meet Standard	Approaches Standard	Meets Standard
Graduates will be able to apply program-specific knowledge to address practical problems using an ethical, evidence-based framework.	Unable to identify or apply relevant program-specific knowledge to practical problems. Solutions are incorrect, irrelevant, or demonstrate a fundamental misunderstanding of the problem context.	Identifies and applies some relevant program-specific knowledge to practical problems, but inconsistencies are evident. Solutions are partially correct and address parts of the problem but may miss key aspects or lack depth.	Consistently identifies and accurately applies relevant program-specific knowledge to practical problems. Solutions are correct, comprehensive, and well-suited to the problem context, demonstrating a thorough understanding of the subject matter.
Graduates will be able to utilize argumentation skills appropriate for a given problem or context.	Demonstrates a lack of understanding of argumentation skills, presenting arguments that are unclear, unsupported by evidence, or irrelevant to the problem or context. Arguments are often illogical or flawed, failing to address the issue effectively.	Demonstrates basic argumentation skills, with arguments that are generally clear and relevant to the problem or context. Some evidence is used, but the connections between evidence and conclusions may be weak or underdeveloped. Arguments may lack depth or coherence, occasionally missing key aspects of the problem.	Effectively utilizes argumentation skills, presenting well-structured arguments that are clear, relevant, and supported by appropriate evidence. The arguments are logical, coherent, and directly address the problem or context. The use of evidence is strong, with clear connections to conclusions, demonstrating a thorough understanding of effective argumentation.
Graduates will be able to construct and implement networks and data management systems that protect intellectual property using cybersecurity principles.	Fails to construct or implement networks and data management systems that protect intellectual property. Designs lack fundamental cybersecurity principles, resulting in systems that are vulnerable to breaches. There is little to no evidence of understanding how to safeguard intellectual property	Constructs and implements basic networks and data management systems with some measures to protect intellectual property. While some cybersecurity principles are applied, the systems may have vulnerabilities and may not fully protect against potential threats. The implementation shows an understanding of cybersecurity principles	Effectively constructs and implements networks and data management systems that robustly protect intellectual property. The designs incorporate comprehensive cybersecurity principles, resulting in secure systems that are resilient against breaches. There is a clear and thorough application of cybersecurity best practices, demonstrating a strong understanding of

		but lacks thoroughness and robustness.	how to safeguard intellectual property.
Graduates will be able to apply information security principles to analyze, detect and mitigate vulnerabilities and intrusions.	Demonstrates an inability to effectively apply information security principles. Analyses are incomplete or incorrect, and detection of vulnerabilities and intrusions is frequently missed. Mitigation strategies are ineffective or absent, showing a fundamental lack of understanding of information security principles	Apply information security principles adequately. Analyses uncover some vulnerabilities and intrusions but may overlook critical issues. Detection mechanisms function to some extent, and mitigation strategies are occasionally effective. However, the overall approach is not comprehensive, potentially leaving some vulnerabilities unaddressed.	Proficiently utilizes information security principles to conduct thorough analysis, detection, and mitigation of vulnerabilities and intrusions. Analyses are detailed and precise, detection mechanisms are dependable and proactive, and mitigation strategies are strong and well-executed. The graduate exhibits a deep understanding of information security principles and applies them consistently to safeguard systems from threats.

2022-2023 Assessment Data

SLO 3: Graduates will be able to construct and implement networks and data management systems that protect intellectual property using cybersecurity prin

Cybersecurity

		Spring 1 2023	Spring 1 2023	Spring 1 2023	Spring 1 2023	Spring 1 2023	Spring 2 2023	Spring 2 2023	Spring 2 2023	Fall 1 2022
		CYBR-5010-12	**CYBR-5010-13**	**CYBR-5010-14**	**CYBR-5010-15**	**CYBR-5020-11**	**CYBR-5030-21**	**CYBR-5030-22**	**CYBR-5030-23**	**CYBR-5220 - 11**
Does Not Meet Standard (0 to 69%)	Fails to construct or implement networks and data management systems that protect intellectual property. Designs lack fundamental cybersecurity principles, resulting in systems that are vulnerable to breaches. There is little to no evidence of understanding how to safeguard intellectual property	15%	0%	9%	0%	0%	0%	0%	13%	0%
Approaches Standard (70 to 89%)	Constructs and implements basic networks and data management systems with some measures to protect intellectual property. While some cybersecurity principles are applied, the systems may have vulnerabilities and may not fully protect against potential threats. The implementation shows an understanding of cybersecurity principles but lacks thoroughness and robustness.	0%	0%	0%	0%	0%	6%	0%	0%	50%
Meets Standard (90 to 100%)	Effectively constructs and implements networks and data management systems that robustly protect intellectual property. The designs incorporate comprehensive cybersecurity principles, resulting in secure systems that are resilient against breaches. There is a clear and thorough application of cybersecurity best practices, demonstrating a strong understanding of how to safeguard intellectual property.	85%	100%	91%	100%	100%	94%	100%	87%	50%
		Introduced	Introduced	Introduced	Introduced	Introduced	Reinforce	Reinforce	Reinforce	Reinforce

Cybersecurity

Fall 1 2022	Spring 1 2023	Spring 2 2023	Spring 2 2023	Summer 1 2022	Fall 1 2022	Spring 2 2023	
CYBR-5220 - 12	**CYBR-5963-11**	**CYBR-5961-21**	**CYBR-5963-21**	**CYBR-5961-11**	**CYBR-5962-11**	**CYBR-5962-21**	**TOTAL**
0%	0%	0%	0%	0%	0%	0%	0%
0%	0%	0%	0%	0%	0%	0%	100%
100%	100%	100%	100%	100%	100%	100%	0%
Reinforce	Evaluated	Evaluated	Evaluated	Evaluated	Evaluated	Evaluated	

2022-2023 Assessment Data

SLO 4: Graduates will be able to apply information security principles to analyze, detect and mitigate vulnerabilities and intrusions.

Cybersecurity

		Spring 1 2023	Spring 1 2023	Spring 1 2023	Spring 1 2023	Spring 1 2023	Spring 2 2023	Spring 2 2023	Spring 2 2023	Spring 2 2023
		CYBR-5000-12	**CYBR-5000-13**	**CYBR-5000-14**	**CYBR-5000-15**	**CYBR-5020-11**	**CYBR-5030-21**	**CYBR-5030-22**	**CYBR-5030-23**	**CYBR-5230-21**
Does Not Meet Standard (0 to 69%)	Demonstrates an inability to effectively apply information security principles. Analyses are incomplete or incorrect, and detection of vulnerabilities and intrusions is frequently missed. Mitigation strategies are ineffective or absent, showing a fundamental lack of understanding of information security principles	15%	0%	9%	0%	0%	0%	0%	13%	14%
Approaches Standard (70 to 89%)	Apply information security principles adequately. Analyses uncover some vulnerabilities and intrusions but may overlook critical issues. Detection mechanisms function to some extent, and mitigation strategies are occasionally effective. However, the overall approach is not comprehensive, potentially leaving some vulnerabilities unaddressed.	0%	0%	0%	0%	0%	6%	0%	0%	0%
Meets Standard (90 to 100%)	Proficiently utilizes information security principles to conduct thorough analysis, detection, and mitigation of vulnerabilities and intrusions. Analyses are detailed and precise, detection mechanisms are dependable and proactive, and mitigation strategies are strong and well-executed. The graduate exhibits a deep understanding of information security principles and applies them consistently to safeguard systems from threats.	85%	100%	91%	100%	100%	100%	100%	87%	86%
		Introduced	Introduced	Introduced	Introduced	Reinforce	Reinforce	Reinforce	Reinforce	Reinforce

Spring 2 2023	Spring 2 2023	Spring 2 2023	Spring 2 2023	Summer 2 2022	Spring 1 2023	Spring 1 2023	Spring 2 2023	Spring 2 2023	Summer 1 2022	Fall 1 2022	Fall 2 2022	
CYBR-5230-22	**CYBR-5230-23**	**CYBR-5230-24**	**CYBR-5230-25**	**CYBR-5240- 11**	**CYBR-5961-11**	**CYBR-5963-11**	**CYBR-5961-21**	**CYBR-5963-21**	**CYBR-5961-11**	**CYBR-5962-11**	**CYBR-5962-21**	**TOTAL**
11%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	4%
0%	0%	13%	18%	0%	0%	0%	0%	0%	0%	0%	0%	2%
89%	100%	88%	82%	100%	100%	100%	100%	100%	100%	100%	100%	94%
Reinforce	Reinforce	Reinforce	Reinforce	Reinforce	Evaluated	Evaluated	Evaluated	Evaluated	Evaluated	Evaluated	Evaluated	

SLO 3: Graduates will be able to construct and implement networks and data management systems that protect intellectual property using cybersecurity principles

	Spring 1 2023	Spring 1 2023	Spring 1 2023	Spring 1 2023	Spring 1 2023	Spring 2 2023	Spring 2 2023	Spring 2 2023	Fall 1 2022	Fall 1 2022	Spring 1 2023	Spring 2 2023	Spring 2 2023	Summer 1 2022
	CYBR-5010-12	**CYBR-5010-13**	**CYBR-5010-14**	**CYBR-5010-15**	**CYBR-5020-11**	**CYBR-5030-21**	**CYBR-5030-22**	**CYBR-5030-23**	**CYBR-5220 - 11**	**CYBR-5220 - 12**	**CYBR-5963-11**	**CYBR-5961-21**	**CYBR-5963-21**	**CYBR-5961-11**
1	D	M	M	M	M	A	M	M	M	M	M	M	M	M
2	M	M	M	M	M	M	M	M	A	M		M	M	M
3	M	M	M	M		M	M	M	M	M		M	M	
4	M	M	M	M		M	M	M	M	M		M	M	
5	M	M	M	M		M	M	M	A	M		M	M	
6	M	M	M	M		M	M	M	A	M			M	
7	D	M	M	M		M	M	M		M			M	
8	M	M	M	M		M	M	M		M			M	
9	M	M	D	M		M	M	M		M				
10	M	M	M			M	M	M		M				
11	M	M	M			M	M	D		M				
12	M	M				M	M	M		M				
13	M	M				M	M	M		M				
14		M				M	M	D		M				
15						M	M	M		M				
16						M	M			M				
17						M	M			M				
18						M				M				
19										M				
20														
21														
22														
23														
24														
25														

D	2	0	1	0	0	0	0	2	0	0	0	0	0	0
A	0	0	0	0	0	1	0	0	3	0	0	0	0	0
M	11	14	10	9	2	17	17	13	3	19	1	5	8	2
TOTAL	13	14	11	9	2	18	17	15	6	19	1	5	8	2

D	15%	0%	9%	0%	0%	0%	0%	13%	0%	0%	0%	0%	0%	0%
A	0%	0%	0%	0%	0%	6%	0%	0%	50%	0%	0%	0%	0%	0%
M	85%	100%	91%	100%	100%	94%	100%	87%	50%	100%	100%	100%	100%	100%

Fall 1 2022	Spring 2 2023
CYBR-5962-11	**CYBR-5962-21**
M	M
	M
	M
	M
	M
	M
	M
	M

Does Not Meet Standard (0 to 69%)
Approaches Standard (70 to 89%)
Meets Standard (90 to 100%)

Stopped participating in course
Did not submit final artifact
Never participated in course

0	0	**5**
0	0	**4**
1	8	**140**
1	8	**149**

0%	0%	**3%**
0%	0%	**3%**
100%	100%	**94%**

SLO 4: Graduates will be able to apply information security principles to analyze, detect and mitigate vulnerabilities and intrusions.

	Spring 1 2023	Spring 1 2023	Spring 1 2023	Spring 1 2023	Spring 1 2023	Spring 2 2023	Spring 2 2023	Spring 2 2023	Spring 2 2023
	CYBR-5010-12	**CYBR-5010-13**	**CYBR-5010-14**	**CYBR-5010-15**	**CYBR-5020-11**	**CYBR-5030-21**	**CYBR-5030-22**	**CYBR-5030-23**	**CYBR-5230-21**
1	D	M	M	M	M	A	M	M	M
2	M	M	M	M	M	M	M	M	M
3	M	M	M	M		M	M	M	M
4	M	M	M	M		M	M	M	M
5	M	M	M	M		M	M	M	M
6	M	M	M	M		M	M	M	D
7	D	M	M	M		M	M	M	M
8	M	M	M	M		M	M	M	
9	M	M	D	M		M	M	M	
10	M	M	M			M	M	M	
11	M	M	M			M	M	D	
12	M	M				M	M	M	
13	M	M				M	M	M	
14		M				M	M	D	
15						M	M	M	
16						M	M		
17						M	M		
18						M			
19									
20									
21									
22									
23									
24									
25									

D	2	0	1	0	0	0	0	2	1
A	0	0	0	0	0	1	0	0	0
M	11	14	10	9	2	17	17	13	6
TOTAL	13	14	11	9	2	18	17	15	7

D	15%	0%	9%	0%	0%	0%	0%	13%	14%
A	0%	0%	0%	0%	0%	6%	0%	0%	0%
M	85%	100%	91%	100%	100%	100%	100%	87%	86%

Spring 2 2023	Spring 2 2023	Spring 2 2023	Spring 2 2023	Summer 2 2022	Fall 1 2022	Spring 1 2023	Spring 2 2023	Spring 2 2023	Summer 1 2022
CYBR-5230-22	**CYBR-5230-23**	**CYBR-5230-24**	**CYBR-5230-25**	**CYBR-5240- 11**	**CYBR-5961-11**	**CYBR-5963-11**	**CYBR-5961-21**	**CYBR-5963-21**	**CYBR-5961-11**
M	M	A	M	M	M	M	M	M	M
M	M	M	M	M	M		M	M	M
M	A-	M	M	M	M		M	M	
M	M	M	M	M	M		M	M	
M	M	M	A		M		M	M	
M	M	M	A		M			M	
M	M	M	M		M			M	
M	M	M	M		M			M	
D	M		M						
	A-		M						
			M						

1	0	0	0	0	0	0	0	0	0
0	0	1	2	0	0	0	0	0	0
8	8	7	9	4	8	1	5	8	2
9	8	8	11	4	8	1	5	8	2

11%	0%	0%	0%	0%	0%	0%	0%	0%	0%
0%	0%	13%	18%	0%	0%	0%	0%	0%	0%
89%	100%	88%	82%	100%	100%	100%	100%	100%	100%

Fall 1 2022	Spring 2 2023
CYBR-5962-11	**CYBR-5962-21**
M	M
	M
	M
	M
	M
	M
	M
	M

Does Not Meet Standard (0 to 69%)
Approaches Standard (70 to 89%)
Meets Standard (90 to 100%)

Stopped participating in course
Did not submit final artifact
Never participated in course

0	0
0	0
1	8
1	8

7
4
168
179

0%	0%
0%	0%
100%	100%

4%
2%
94%