STUDENT LEARNING ASSESSMENT PROGRAM SUMMARY FORM AY Fall 2024 SP 2025

Please complete a separate worksheet for each academic program (major, minor) at each level (undergraduate, graduate) in your department.

Degree and Program Name: MS in Cybersecurity

Submitted By: Dr. Rigoberto Chinchilla,
Graduate Coordinator

PART ONE

What are the learning objectives?	How, where, and when are they assessed?	What are the expectations?	What are the results?	Committee/ person responsible? How are results shared?
1. Assess, by analyzing technical and operational requirements, and enterprise level information cybersecurity system. **COVERS: CGS Learning Goal "A depth of Content Knowledge"** **COVERS: CGS Learning Goal "Critical thinking and Problem-Solving Skills"** **COVERS: CGS Learning Goal "Evidence of Advanced Scholarship through research and/or creative activity"** **COVERS: CGS Learning Goal "Effective Oral Communication Skills"**	Students are assessed during the final Capstone activity by building cybersecurity protections according to specifications. Students work around practical problems and assess the technical and operational cybersecurity needs of the Information System. Each student is encouraged to present a possible solution to the problem, and all the solutions are discussed in group and implemented as a team. The solution Typically require an integration of skills and concepts covered during the program and a high degree of Critical thinking abilities.	Students are expected to pass the Capstone Experience (formerly to graduate from the program which requires students to demonstrate their technical and critical thinking skills and the ability to communicate orally when working in group) Expectations are: - 5 percent exceed the expectations - 90 percent meet expectations - 5 percent do not meet expectations	a. Direct Measures: Out of a total of 35 students who completed their Capstone Experience in FALL 2024, SPRING 2025, 100% (~35 students) met expectations; 0% (0 students) exceeded expectations; and 0% (0 student) failed to meet expectations. a. Indirect Measures: All students wrote a comprehensive paper of their expectations of the program and the capstone, their oral communication skills within the activities in the capstone were rated superior (excellent technical oral communications)	Results are shared with graduate faculty and with the Graduate Committee to continuously improve the program. The Graduate Faculty at least once a year feedback and suggest recommendations to the program and how to continuously improve critical thinking within our graduate programs.

			while written communication skills were rated 4.0 in the scale of 5.0 (5 being the highest and 1 being the lowest) All students are currently employed in companies ranging from Google, Cisco, AT&T, Amazon, and many local companies.	
2. Construct the architecture of a typical cybersecurity system; identify significant vulnerabilities, risks, and points at which specific security technologies/methods should be employed **COVERS: CGS Learning Goal "A Depth of Content Knowledge"** **COVERS: CGS Learning Goal "Effective Written Communication Skills"**	a. Direct Measures: "TEC 5553 (Cybersecurity) and CYB 5900 (CAPSTONE) are two required courses with close to 40 (one to two hours long) laboratory practices specifically designed to provide students with the cybersecurity tools to identify significant vulnerabilities, risks and points at which specific security technologies/methods should be employed. Each experiment and laboratory practice must be successful for the student to approve of the course. The instructor has designed labs to stimulate critical thinking abilities related to cybersecurity defense. The hands-on component of the program is specifically built to produce either working or not working conditions of the cybersecurity system. Each student must tune the systems to a 100% operational or no grade is assigned. b. Indirect Measures:	The expectation is that 100% of the students must achieve 100% of the challenges posed by the 40+ practices aimed at building different architectures of cybersecurity systems. If a student cannot finish or can't implement the systems, instructors will guide them until they are able to do it. A second expectation is to measure the ability of the students to write a technological paper. The courses TEC 5413, TEC 5333 and CYB 5900 (CAPSTONE) require writing at least half-dozen extensive professional research papers in the fields of Biometric security and Cybersecurity in general. Expectations: - 5 percent will exceed expectations - 90 percent meet expectations	a. Direct Measures: Out of 35 students enrolled in classes in Fall 2024 and SP 2025 and SUMMER 2025, about 35 students met expectations because you can't move to the next practice until a previous practice /design is successful. Therefore, we assure all of them have successful practices. However, just about 30 students were able to finish the challenges without help (~85%) and the rest needed partial or a lot of help from instructors until they completed their designs. b. Indirect Measures: Again, our most valuable indirect measure at this point is the fact that 100% of them get a position in the field before graduation or within 6 months after graduation.	The Cybersecurity Faculty in Constant Communication is responsible for the implementation of this objective through many courses in the program. The whole program is checked every semester with the leadership of the cybersecurity graduate coordinator.

	All our graduates so far have got a job in the field within 6 months of graduation. Not only are they employed almost immediately but they are employed by prestigious companies in the field.	- 5 percent will not meet expectations on intellectual research		
3. Conduct network penetration tests, troubleshoot, and implement attack countermeasures in a typical information system **COVERS: CGS Learning Goal "A Depth of Content Knowledge"** **COVERS: CGS Learning Goal "Effective Written and Oral Communication Skills"** **COVERS: CGS Learning Goal "Critical thinking and Problem-Solving Skills"**	a. Direct Measures: "TEC 5553 (Cybersecurity), MIS4860 (Ethical Hacking) MIS 4850 (Systems security) and CYB 5900 (CAPSTONE) are four required courses with close to 50 (one to two hours long) laboratory practices specifically designed to provide students with the cybersecurity tools to conduct network penetration tests, troubleshoot, and implement attack countermeasures in a typical information system Each experiment and laboratory practice must be successful for the student to approve of the course. The instructor has designed labs to stimulate critical thinking abilities related to cybersecurity defense. The hands-on component of the program is specifically built to produce either working or not working conditions of the cybersecurity system. Each student must tune the systems to a 100% operational or no grade is assigned. b. Indirect Measures:	The expectation is that 100% of the students must make 100% of the challenges posed by the 50+ practices aimed at building different architectures of cybersecurity systems. If a student cannot finish or can't implement the systems, instructors will guide them until they are able to do it. A second expectation is to measure the ability of the students to write a technological paper. The course TEC 5413, TEC 5333 and CYB 5900 (CAPSTONE) require writing extensive research professional papers (At least half a dozen) in the fields of Biometric security and cybersecurity in general. Expectations: - 5 percent will exceed expectations - 90 percent meet expectations - 5 percent will not meet expectations on intellectual research We expect that our students not just perform well in their	a. Direct Measures: Out of 35 students enrolled in the class in FALL 2024, Summer 2025, SPRING 2025, just about 30 students met expectations because you can't move to the next practice until a previous practice /design is successful. Therefore, we assure all of them have successful practices. However, just about 25 students were able to finish the challenges without help (~72%) and the rest needed partial or a lot of help from instructors until they complete their designs. b. Indirect Measures: Again, our most valuable indirect measure at this point is the fact that 100% of them get a position in the field before graduation or within 6 months after graduation.	The Cybersecurity Faculty in Constant Communication is responsible for the implementation of this objective through many courses in the program. The whole program is checked every semester with the leadership of the cybersecurity graduate coordinator.

	All our graduates so far have got a job in the field within 6 months of graduation. Not only are they employed almost immediately but they are employed by prestigious companies in the field.	jobs but excel professionally in the companies they are hired by. Although it is difficult to measure because with a few exceptions they tend not to communicate with EIU or the professor. The few who do communicate with us exceeded expectations. I am planning to design a system for the next graduates to have more formal feedback from them a year after the employment started.		
4. Identify the components of cybersecurity layered structure for: a. Network defense architecture b. Access control and auditing c. Continuous network monitoring d. Real-time security solutions. **COVERS: CGS Learning Goal "A Depth of Content Knowledge"** **COVERS: CGS Learning Goal "Critical thinking and Problem-Solving Skills"**	Direct Measures: TEC 5413 (Advanced Data telecommunications) TEC 5353 (Cybersecurity) CYB 5900 (Capstone) MIS 4850 (System Security) MIS 4860 (Ethical Hacking) TEC 6363 (Database Security) These courses are specifically designed to teach (theoretically and hands on) to identify the components of a cybersecurity layered structure, network defense architecture, access control and auditing, Continuous network monitoring and real time security solutions are also integral parts of these courses. Typical Assignments include to implement real time security Solutions with commercial equipment, program highly advanced Cyber-equipment to defend the network and Homework assignments requiring to identify all	Students are expected to demonstrate their ability to Identify the components of cybersecurity layered structure for, network defense architecture, access control and auditing, Continuous network monitoring, and real time security solutions. Expectations are: Twenty percent will exceed expectations. Seventy percent will meet expectations. Ten percent will not necessarily meet expectations.	a. Direct Measures: Out of a total of 35 students in the class in FALL 2024, Summer 2025, SPRING 2025 just about 30 students met expectations due to the fact that you can't move to the next practice until a previous practice /design is successful. Therefore, we assure all of them have successful practices. However, about 25 students were able to finish the challenges without help (~72%) and the rest needed partial or a lot of help from instructors until they completed their designs. b. Indirect Measures: Out of a total of 35 students who returned The Capstone graduate surveys at the end of the program, Our students were very candid and provide constructive comments as well excellent	The Cybersecurity Faculty in Constant Communication is responsible for the implementation of this objective through many courses in the program. The whole program is checked every semester with the leadership of the cybersecurity graduate coordinator.

	components of a cybersecurity layered structure		recommendations for the program, over all the level of satisfaction was higher than expected for a new program.	
5. Describe and apply the fundamental and advanced technologies, components, and issues related to communications, data networks, and information systems. **COVERS: CGS Learning Goal "A Depth of Content Knowledge"** **COVERS: CGS Learning Goal "Critical thinking and Critical Thinking Skills"** **COVERS: CGS Learning Goal "Evidence of Advanced Scholarship through research and/or creative activity"**	a. Direct Measures: - TEC 5313 (Advanced Data Telecommunications) - TEC5333 or MBA 5670 (Information systems) - TEC 5323 (Advanced Databases) - TEC 5353 (Cybersecurity) - MIS 4850 (Systems Security) These courses are specially designed for describing and applying the fundamental and advanced technologies, components, and issues related to communications, data networks, and information systems.	Expectations are: - 10 % will exceed expectations - 85 % meet expectations - 5 % do not meet expectations regarding the impact of global technology We expect that our students not just perform well in their jobs but excel professionally in the companies they are hired. Although it is exceedingly difficult to measure because with a few exceptions they tend not to communicate with EIU or the professor. The few who do communicate with us exceeded expectations. I am planning to design a system for the next graduates to have more formal feedback from them a year after the employment started.	Direct Measures: out of 35 students in the class in FALL 2024, Summer 2025, SPRING 2025 about 30 students met expectations because you can't move to the next practice until a previous practice /design is successful. Therefore, we assure all of them have successful practices. However, about 25 students were able to finish the challenges without help (~72%) and the rest needed partial or a lot of help from instructors until they completed their designs. Indirect measures: -TEC 5313 (Advanced Data Telecommunications) -TEC533 or MBA 5670 (Information systems) -TEC 5323 (Advanced Databases) - TEC 5353 (Cybersecurity) - MIS 4850 (Systems Security) Are the foundations for all other courses in the program therefore the average performance in subsequent courses is an indirect measure of how well the foundation was taught.	The Cybersecurity Faculty in Constant Communication is responsible for the implementation of this objective through many courses in the program. The whole program is checking every semester with the leadership of the Cybersecurity graduate coordinator.

6. Analyze network designs, topologies, architectures, protocols, communications, administration, operations, and resource management, for wired and wireless networks that affect security of the cyberspace. **COVERS: CGS Learning Goal “A Depth of Content Knowledge”** **COVERS: CGS Learning Goal “Critical thinking and Critical Thinking Skills”**	Direct Measures: TEC 5413 (Advanced Data telecommunications) TEC 5353 (Cybersecurity) CYB 5900 (Capstone) MIS 4850 (System Security) TEC 6363 (Database Security) These courses are specifically designed to teach (theoretically and hands too. Identify the components of cybersecurity layered structure for, network defense architecture, access control and auditing, Continuous network monitoring, and real time security solutions.	Students are expected to. Analyze network designs, topologies, architectures, protocols, communications, administration, operations, and resource management, for wired and wireless networks that affect security of the cyberspace. Expectations are: 20% will exceed expectations. 70% will meet expectations. 10% will not necessarily meet expectations. We expect that our students not just perform well in their jobs but excel professionally in the companies they are hired by. Although it is very difficult to measure because with a few exceptions they tend not to communicate with EIU or the professor. The few who do communicate with us exceeded expectations. I am planning to design a system for the next graduates to have more formal feedback from them a year after the employment started.	b. Direct Measures: Out of a total of 35 students in the class in FALL 2024, Summer 2025, SPRING 2025 just about 30 students met expectations due to the fact that you can’t move to the next practice until a previous practice /design is successful. Therefore, we assure all of them have successful practices. However, about 25 students were able to finish the challenges without help (~72%) and the rest needed partial or a lot of help from instructors until they completed their designs. b. Indirect Measures: Out of a total of 35 students who returned The Capstone graduate surveys at the end of the program. Our students were very candid and provide constructive comments as well excellent recommendations for the program, over all the level of satisfaction was higher than expected for a new program.	The Cybersecurity Faculty in constant communication is responsible for the implementation of this objective through many courses in the program. The whole program is Checked every semester with the leadership of the cybersecurity graduate coordinator. We have hold two meetings during each semester with the two major responsible faculty of the program (Dr. Chinchilla and Dr. Ilia)

Covers CGS learning goal “ETHICS AND PROFESSIONAL RESPONSIBILITY”	The Cybersecurity Field is if not the most important, one of the most important fields where Ethic principles have a lot to do with the proper implementation of cybersecurity measures. It is so important that we have dedicated one full semester course just to this issue on the course. MIS 4860 “Ethical Hacking” In addition to this course, complete sections on ethics are covered in two more courses. -TEC 5333/MBA 5670 (Management of Computer technologies) (A complete week is devoted to Ethic issues) -TEC 5353 (Cybersecurity): Also, a complete week is devoted to Ethic issues) -TEC 5413 (Biometric Security) were ethical societal issues of implementing biometrics technologies are explored. They must summarize extensive articles about the subject. Ethics is married to Cybersecurity, it could not be Cybersecurity without proper professional Ethics, indeed our students have basic training in	Students are expected to demonstrate their ability to Identify ethical issues when designing cybersecurity including Biometric Systems and the components of cybersecurity layered structure for, network defense architecture, access control and auditing, Continuous network monitoring, and real time security solutions. Expectations are: Twenty percent will exceed expectations. Seventy-five percent will meet expectations. Five percent will not necessarily meet expectations.	Direct Measures: Out of a total of 35 students enrolled in courses (FALL 2024, SPRING 2025, summer 2025) -15% exceeded the expectations. -75% met expectations. -10% did not meet expectations. These conclusions were based on grade averages of our students in those courses. Indirect Measures: Out of a total of about 35 students who returned The Capstone graduate surveys at the end of the program. Our students were very candid and provide constructive comments as well excellent recommendations for the program, over all the level of satisfaction was higher than expected for a new program	The Cybersecurity Faculty in reasonable Communication is responsible for the implementation of this objective through many courses in the program. The whole program is Check every semester with the leadership of the cybersecurity graduate coordinator. We have held two meetings during each semester with the two major responsible faculty of the program (Dr. Chinchilla and Dr. Ilia)

	the development of ethical programs in companies related to cybersecurity.			

PART TWO

Describe your program's assessment accomplishments since your last report was submitted. Discuss ways in which you have responded to the CASA Director's comments on last year's report or simply describe what assessment work was initiated, continued, or completed.

This is the third program assessment.

- The CGS learning Goals have been maintained/strengthened with the Program objectives.
- Expectations of Learning Objective 6 have been maintained/strengthened.
- Examples of kind of assignments that fulfill the objectives have been included in the report.
- Expectations of post-graduate employment have been included.
- Meetings between the two main responsible faculty of the program (teaching most of the key courses) has been held to discuss the program improvements (For Example Dr. Illia and D. Chinchilla promoted EIU as an institution to have a legal agreement and a partnership with the EC council, one of the leading Cybersecurity Certifications companies in the USA, we now have direct access to all their materials and certification courses)
- An ongoing research project is being build that will revolutionize the teaching of cybersecurity: A real Network (connected to the world) that will be receiving real attacks from unknown hackers around the world. ITS personnel will be invited to check the full independence of this network from the EIU network or equipment. This will allow us to have a real-world experience analyzing real attacks with real hackers. The project is expected to be completed by May 2026.

PART THREE

Summarize changes and improvements in ***curriculum, instruction, and learning*** *that have resulted from the implementation of your assessment program. How have you used the data? What have you learned? In light of what you have learned through your assessment efforts this year and in past years, what are your plans for the future?*

The major changes in the M.S. in Cybersecurity have been related to changes in cybersecurity technologies throughout the last four years. Our courses must be constantly evolving to reflect those changes. Also, we have developed/modified at least one dozen new laboratory practices to accommodate those changes and challenges in cybersecurity. The MS. n Cybersecurity collaborates with the MS in Technology program, providing several cybersecurity courses not only to MS. In Cybersecurity students but also to MS in Technology students. The cybersecurity field is now a core content offered by the School of Technology courses. One major challenge that raised this year is the need of an additional Faculty devoted to teaching Cybersecurity related courses.

Fortunately, due to the advances in Cloud Computing and remote learning, we have now eliminated the need to spent time in our facilities (Except for some international students that due to Visa issues they must be taking courses on campus) We were able to eliminate the residency requirements of the program. An intense and deep collaboration between ITS and our Program has led to the possibility of 100% remote practices. However, ITS in 2024 upgraded the system and a significant investment rounding many thousands of dollars is need for this purpose. The upgrade of equipment (cloud) hosted by ITS (about every three years) is supported with student's fees.

.

Unfortunately, there are still four areas we are not covering in this important field: CYBERSECURITY FORENSICS, CLOUD SECURITY and PENETRATION TESTING and CYBERSECURITY COMPLIANCE. It is extremely difficult to find Faculty in the Cybersecurity area and there are no signs that another unit, A or B, will be approved to cover this deficit soon. We will keep trying to find the right one to revitalize these key areas. Studies in this area will significantly enhance program offering in the field.

We have quickly responded to the demand for flexibility by adapting our course rotations and allowing students to have different options according to their particular interest. As an example, some students wanted to focus on Wed Development and Programming/Coding Security, and we use the current courses of the MS in Technology to offer this flexibility. The major recommendations for the program are the same for the last year and comprise the following four areas:

Cloud Cybersecurity Based Systems
Cybersecurity Forensics
Penetration Testing
Cybersecurity Compliance According to ISO Standards

We believe the program is still lacking behind in these four areas and we are looking for ways how to incorporate these areas within our existing courses or to create new courses to improve our program yet, the resources are scarce, especially in the area of new faculty.

The program has not changed much since its creation in terms of courses offered, however the courses has been updated properly to reflect the new challenges, but without fulfilling the previous 4 areas (or at least two of those areas) our program might become obsolete in the next five years.

1. Assessment Drives New Curriculum Development and Content Update

A key innovation is to have designed a cloud-based laboratory for the program. Using VMWARE, cloud computing and virtual images of the equipment in our laboratory, we migrated to a cloud-based laboratory that is fully operational right now.

Regarding Cloud Base Cybersecurity Based Systems as well Cybersecurity Compliance, we still need to prepare a faculty or hire a new one that can cover these areas of expertise, which was planned for year 2024 yet EIU did not authorize the new hire. Discussions continually take place within the areas of all areas of the program.
Every November for the last 5 years we have celebrated the "cybersecurity day" at which we invite professionals in the field of cybersecurity to share their experience with our students. In Fall 2024 2 professionals from GOOGLE (Alumni of the program) came to campus to share their experiences in the field.

This September (2025) the "Student cybersecurity Club" was formed, they are working in the new project (To have a worldwide network that can he hacked, to study the behavior and techniques of hackers)

2. Assessment Drives Improvement in Instruction and Learning

Cybersecurity is one of the areas where it is difficult to keep the pace between what is going on in the real market/companies with what is taught in the classroom. However, we keep in close contact with about 6 students working at AMAZON, GOOGLE, and CISCO to let us know their suggestions to keep our program up to date. We encourage faculty to update books, update content, and overall keep familiar with the new challenges in cybersecurity for continuous improvement. The Graduate Faculty in the MS in Cybersecurity keeps continuous discussions and communication to improve every course in the program. During the past academic year, course contents and delivery approaches have been updated for the graduate program. Instructors are responsible for constant improvement in their preparation and delivery of the subject. Based upon students' interests and responses to the contents, adjustments have been made to meet students' needs. As a result, teamwork and class interaction have been strongly promoted in the program. One of the major signs that we keep the pace with the necessary improvements in learning in reflected in the course "CYB SEMINAR" we MUST teach the latest certification exam contents (which is typically upgraded by experts in the field every two years) the two certifications we promote CompTIA sec+ and CISSP must be upgraded according to the needs of the market and we follow these upgrades very closely.

3. Assessment Drives Improvement in Capstone Experience

As a part of graduation requirement, a Capstone Experience is required, graduate students with non-thesis option are required to complete a Capstone Experience. The Capstone Experience has served the purpose of assessing students' ability to integrate their knowledge and skills gained during their graduate study to solve cybersecurity challenges. The importance of meeting security specifications and working in groups to set up a cybersecurity protection system has been highlighted in the Capstone Experience process, as an integral part of the graduate study in Cybersecurity.   The Graduate Committee addressed the possibility of continuously improving the final Capstone Experience.

Although it is not called capstone CYB 5550 (cybersecurity Seminar) is a course aimed at motivating our students to obtain two professional certifications

- COMTIA SECURITY +
- CISSP

Although not classified as a capstone formally, this course helps to integrate all the theoretical courses into an integral vision of the field. We can think of CYB 5550 as a theoretical Capstone and TEC 5900 as the Hands-on capstone. Both courses shape potential deficiencies in theoretical and practical areas the students might have missed in their course work. This course is taught collaboratively by two faculty, each one certified in the previous certifications.

In summary the combo CYB 5900 and CYB 5500 act as round and solid capstone experience for our students. By necessity both courses must be u0pdated yearly to be in tune with the market needs. For example, the certification material expires automatically every two years, so we must keep up the pace with the new demands.

4. Students and Employers Are Highly Satisfied with Their Educational Experience and Outcome.

As a result of high-quality education, students are highly satisfied by their overall experience in the MS in Cybersecurity program. By the time they take the capstone experience most students are graduating in the same semester. A satisfaction survey is conducted with every student who is graduating for satisfaction feedback purposes and suggestions. For example, during Summer 2025, Fall 2024 and Spring 2025 semesters, they described their interaction with faculty as excellent. They rated the faculty expertise and teaching competency very good. They regarded their overall experience in their graduate education as excellent. Positive word of mouth by our current and past graduates has become the most effective way for us to recruit new applicants to the program.

We need to improve in this area, we do not know how satisfied employers are with our students, we only know that our students are getting excellent positions in top notch companies in cybersecurity. Our long-term measurements are measured by the rate of success of our alumni in top-notch private companies.