Cybersecurity Annual Assessment 2023-2024

Annual Assessment 2023-2024

Cybersecurity

Program Profile

Program Mission Statement
Please insert your program mission statement here

William Woods University's business programs provide an exceptional learning environment that empowers students to succeed as they continue their education or pursue professional endeavors. The cybersecurity program is designed around identified core knowledge areas supporting information security. The program prepares students to enter the IT and cybersecurity workforce or continue their education in a professional graduate degree program.

Program Data

Delivery Method

Traditional On Campus
Online
Hybrid (selected)

Students Majors 2023-2024

49

Student Majors 2022-2023

15

Student Minors 2023-2024

3

Student Minors 2022-2023

Concentrations 2023-2024
If your program contains concentrations, please list the concentrations and the number of students identified within each concentration.

N/A

Concentrations 2022-2023
If your program contains concentrations, please list the concentrations and the number of students identified with each concentration.

N/A

Student Demographics
What are the program goals for student retention, persistence, and degree completion? What do the persistence numbers mean to the faculty in the program? Are the persistence numbers what the program expected? If not, how could the numbers improve?

The Cybersecurity progam has been offered online since 2018 (5 years) and for 2 years on-ground (since Fall 2022). As we continue to enroll students and develop data points on initial retention, persistence and degree completion percentages (first graduates pending), we will be better able to identify trends and establish expectations.

The Cybersecurity department is pleased with the student retention, persistence, and degree completion from this reporting period. Enrollment in the Cybersecurity major increased from 15 to 49 between Fall 2022 and Fall 2023. (These increased from 6 to 10 and 9 to 39 in on-ground and online modalities, respectively during this period). From the available data for First Time Full Time Freshmen (Fall 2022-Fall 2023) 100% of the Cybersecurity majors in that category were retained within the University, within the Department, and within the Major.

Two on-ground students graduated in April 2024. The on-ground program has met with 8 prospective students during this academic year. Prospective student numbers are good in the second full year of the program being offered on-ground. The program has established a dedicated Cybersecurity computer lab (Burton 109) on campus to accommodate the growth of the major.

Areas where we would next like to shift our focus are increasing enrollment of women within the Cybersecurity program. Currently the program consists of 65.31% male students, 30.61% female students, and 4.08% of students that identified as other genders. Increased recruitment efforts can be coordinated to address this and help increase enrollment of women in the program.

The CSS 210 - Introduction to Cybersecurity course is also planned to be offered on Mondays and Fridays from 11:00 am to 12:15 pm during the Spring 2025 term to allow Missouri Military Academy (MMA) students to come to campus to take the on-ground course alongside William Woods University's students.

Optimal Enrollment
Considering current human and physical resources, what is the optimal enrollment for the program?
150

Is the Program Externally Accredited

Yes
No (selected)

External Accreditation
Name the Accrediting Agency or entity including the last review/approval. Is there an accrediting body for the field of study? If yes, what is the name of the group. Is the program seeking accreditation? If no, why?

The program is designed to meet the NSA accreditation requirements and when the program is eligible, this distinction will be sought.

Admissions and Marketing Materials
Reflect on the current marketing materials used for the program. Please attach screen shots of the website or any material you are referencing in this section. What changes, if any, should be made to the material? Are there recommendations on how to modify the current material?

A fact sheet and webpages exist for the Cybersecurity program, and we have provided information for the Marketing department to develop an updated flyer (drafts attached). Modifications to the Cybersecurity webpages have been submitted to the Marketing department in a change request form in the past to be updated to reflect both the on-ground and online programs and the addition of the cybersecurity minor. (Changes are still pending as of 5/5/24). Nina and Paul approved the new flyer design created by Marketing in November 2023 that reflected the online program information but did not see a final draft of the on-ground flyer/fact sheet that is intended to use the same format.

Video testimonies from current students and faculty would improve the webpage.

Marketing Material

Cyber_marketing_materials.docx
Cyber_Flyer.pdf
Cybersecurity_Program_Sheet_proof__old_.pdf
Cybersecurity_Program_Sheet_Proof_Online__new_.pdf

Program Assessment

Standard/Outcome

Identifier	Description
WWU2021.1	Knowledge and Scholarship: Demonstrate current knowledge and educational expertise in an academic or professional discipline engaging students in the process of academic discovery.

Additional Standards/Outcomes

Identifier	Description
CSS.1	Discuss the impact of cybersecurity on society and organizations.
CSS.2	Develop presentations and documentation to communicate technical content.
CSS.3	Describe the process of designing a computer system.
CSS.4	Design and implement cybersecurity solutions based on a set of requirements.
CSS.5	Identify and compare computer networks and architectures.
CSS.6	Communicate computer security principles and their application.

Alignment to the Institutional Objectives
Please discuss the Program alignment to the Institutional Objectives. Specific evidence is not to be uploaded, but discussion is expected of the assignment, and intentionality of how the objective is met with program curriculum.

This program offers a technical education that is specific to the IT industry. Program objectives align with current Univeristy objectives as follows.

CSS 1 to Knowledge and Scholarship, Inclusion, and Intellectual Inquiry.

- Demonstrated through online discussion board assignments, in-class reflection discussions, projects/presentations given to peers and outside stakeholders (such as Symposium presentations and Cybersecurity Awareness Month materials), and activities where students are encouraged to share information with one another or explain concepts to one another.

CSS 2 to Knowledge and Scholarship, Inclusion, Creativity, and Intellectual Inquiry.

- Demonstrated through presentations curated for audiences from end users to cybersecurity teams to C-Suite executives, hosting events and creating materials for campus for Cybersecurity Awareness Month, and collaborative game-based and project-based learning activities.

CSS 3 to Knowledge and Scholarship and Intellectual Inquiry.

- Demonstrated through developing UML (unified modeling language) diagrams for a unique software application design and developing network diagrams for simple computer networks.

CSS 4 to Knowledge and Scholarship and Intellectual Inquiry.

- Demonstrated through CISO (Chief Information Security Officer) Cybersecurity Program Implementation Plans/Whitepapers, Risk Registers, and Cloud Security tool implementation activities.

CSS 5 to Knowledge and Scholarship.

- Demonstrated through TestOut Network Pro computer networking labs (Local Area Networks, Wide Area Networks, Wireless Local Area Networks, etc.), Cloud service labs (Amazon Web Services), and TryHackMe labs (Intrusion Prevention and Intrusion Detection Systems, Firewalls, etc.).

CSS 6 to Knowledge and Scholarship, Inclusion, Creativity, and Intellectual Inquiry.

- Demonstrated through developing sample phishing emails and using social engineering techniques to understand phishing attempts, developing Cybersecurity Awareness Month materials, developing simple network diagrams and connecting SANS CIS Security controls to the network specified and researching how to develop a malware sandbox environment and presenting the findings at the Symposium.

Institutional_objectives_2.docx

General Education Alignment to Program
How do the General Education criteria align with Program Objectives? What courses within the program build upon skills learned from general education courses (please list the program course and the general education criteria)?

CSS.1: Discuss the impact of cybersecurity on society and organizations.

Aligns with: Cultures and Communities (-U), Historical Perspective (-H), Written Communications (-W), Oral Communications (-O), Information Literacy (-i), and Inquiry and Analysis (-Q) courses.

CSS.2: Develop presentations and documentation to communicate technical content.

Aligns with: Natural Science (-N), Math (-M), Information Literacy (-i), Expression and Invention (-X), Written Communications (-W), and Oral Communications (-O) courses.

CSS.3: Describe the process of designing a computer system.

Aligns with: Natural Science (-N), Math (-M), and Inquiry and Analysis (-Q) courses.

CSS.4: Design and implement cybersecurity solutions based on a set of requirements.

Aligns with: Natural Science (-N), Math (-M), Information Literacy (-i), Expression and Invention (-X), Written Communications (-W), and Oral Communications (-O) courses.

CSS.5: Identify and compare computer networks and architectures.

Aligns with: Natural Science (-N), Math (-M), and Inquiry and Analysis (-Q) courses.

CSS.6: Communicate computer security principles and their application.

Aligns with: Natural Science (-N), Math (-M), Information Literacy (-i), Written Communications (-W), and Oral Communications (-O) courses.

Courses in the program that build upon the skills learned in general education courses include the following:

Quantitative Inquiry (Natural Science (-N) and Math (-M) courses)

CMJ 385 Digital Evidence and Forensic Investigations
CMJ 440 Cybercrime and Information Warfare
CMJ 447 Information Security
CSS 210 Introduction to Cybersecurity-Q
CSS 324 Cybersecurity & Internet Architecture
CSS 325 Cyber Attacks and Defenses
CSS 401 Encryption Techniques
CSS 410 Social Engineering
CSS 420 Critical Infrastructures
CSS 440 Cloud Security
MIS 250 Networking
MIS 225 Database Management Systems
MIS 425 Enterprise Systems
MIS 450 Systems Analysis

These courses benefit from the critical thinking, analytical skills, identification of patterns, and logical reasoning presented in the general education classes as they focus on technical systems, some math-based topics like cryptographic algorithms and binary to hexadecimal number conversions, and other quantitative information related to cyberattacks. Additionally, working through processes like the scientific method can help reinforce working through Cybersecurity-related processes such as the NIST Cybersecurity Framework functions or incident response processes.

Communications (Written Communications (-W) and Oral Communications (-O) courses)

CMJ 385 Digital Evidence and Forensic Investigations
CMJ 440 Cybercrime and Information Warfare
CMJ 447 Information Security
CSS 210 Introduction to Cybersecurity-Q
CSS 310 Cybersecurity Law & Ethics
CSS 324 Cybersecurity & Internet Architecture
CSS 325 Cyber Attacks and Defenses
CSS 401 Encryption Techniques
CSS 410 Social Engineering
CSS 420 Critical Infrastructures
CSS 440 Cloud Security
CSS 490 Cybersecurity Capstone
MIS 100 Cloud Computing-Q
MIS 250 Networking
MIS 225 Database Management Systems
MIS 350 Project Management
MIS 425 Enterprise Systems
MIS 450 Systems Analysis

These courses benefit from the written and oral communications skills presented in the general education classes as the cybersecurity industry requires a high level of soft skills in addition to technical skills on a day-to-day basis. Students who will go on to work in the cybersecurity industry will need the foundational skills to write documentation and reports, create training materials, give presentations, and communicate information to different audiences (end users to C-Suite to cybersecurity teams).

Cultures and Communities (-U), Expression and Invention (-X), and Historical Perspective (-H) courses

CSS 210 Introduction to Cybersecurity-Q
CSS 310 Cybersecurity Law & Ethics
CSS 324 Cybersecurity & Internet Architecture
CSS 325 Cyber Attacks and Defenses
CSS 490 Cybersecurity Capstone
MIS 350 Project Management
MIS 425 Enterprise Systems
MIS 450 Systems Analysis

These courses benefit from the creative skills and connections that are drawn in the general education classes by applying them to interconnected computer systems and assisting students in developing their own systems. Additionally, having knowledge of how information systems and technologies were developed and how individuals and societies interacted with them further contextualizes topics covered in these courses.

Information Literacy (-i)

CMJ 385 Digital Evidence and Forensic Investigations
CMJ 440 Cybercrime and Information Warfare
CMJ 447 Information Security
CSS 210 Introduction to Cybersecurity-Q
CSS 310 Cybersecurity Law & Ethics
CSS 324 Cybersecurity & Internet Architecture
CSS 325 Cyber Attacks and Defenses
CSS 401 Encryption Techniques
CSS 410 Social Engineering
CSS 420 Critical Infrastructures
CSS 440 Cloud Security
CSS 490 Cybersecurity Capstone
MIS 100 Cloud Computing-Q
MIS 250 Networking
MIS 225 Database Management Systems
MIS 350 Project Management
MIS 425 Enterprise Systems
MIS 450 Systems Analysis

These courses benefit from the information literacy skills presented in the general education classes as information in technology-based fields is rapidly changing and students need to have the ability to vet sources for relevance and accuracy. Developing data literacy is another important skill that students can gain from these classes along with best practices for research and critical thinking skills.

Inquiry and Analysis (-Q):

As of this reporting period, the CSS 210 - Introduction to Cybersecurity-Q and MIS 100 - Cloud Computing-Q courses are also general education classes under the new general education framework (Inquiry and Analysis -Q category).

NSSE Objectives Discussed Spring 2022

Program Alignment to NSSE Objectives
Faculty discussed the most recent NSSE results in spring of 2022 and identified universal objectives for all academic content. Please articulate what the program is doing to further students' knowledge and skills in the following areas: 1C- Explained course material to one or more students; 2E - Tried to better understand someone else's view by imagining how an issues looks from his/her perspective; 4C-Analyzing an idea, experience, or line of reasoning in depth by examining its parts; 4D- Evaluating a point of view, decision, or information source. Please describe the activities used and the impact on student learning.

Interdisciplinary work in the major focuses on cyber, management information and criminal justice coursework. General education and other such interdisciplinary cousrework occur outside the core major courses.

This program connects learnining to current issues in IT and cybersecurity. Courses such as Cyber Attacks and Defences, Critical Infrastructures and Cybercrime and Information Warfare draw upon major issues found in the information security realm and that impact society as a whole.

This program is designed to meet the National Security Agency Center of Academic Excellence in Cyber Defense and coursework focuses on meeting the requirments for this designation.

1C -

- The CSS 325 - Cyber Attacks and Defenses on-ground course developed and presented Mini Expert Presentations for their final project. (Throughout the class, students worked through a 30-task capture the flag (CTF) cybersecurity challenge that covered a wide range of topics and documented their process through write ups of each lab). From this CTF, students had to choose a topic covered in one of the labs to conduct additional research and expand upon so they could present as an “expert” on the topic for the class.
- Students in the on-ground CSS 210 - Introduction to Cybersecurity course developed Lunch and Learn presentations on a cybersecurity topic of their choice and presented them to the class. Additionally, they created an interactive component for the Lunch and Learn (quiz, game, structured discussion, etc.) that reinforced the topic that they presented on.
- MIS 425 - Enterprise Systems on-ground students developed Splunk Data Dashboards in small groups of 2-3. The groups had to choose the topic of their dashboards, decide how and where they would obtain their dataset, import the data into Splunk, develop 4 visualizations, and then present to their peers on their process and what their dashboards displayed during the practice presentation for the Symposium.

2E -

- Also briefly covered in the CSS 210 Lunch and Learn presentations, students had to consider various audiences (technical, non-technical, etc.) and what information would be pertinent in conveying their chosen topic. Students provided additional descriptions and/or definitions of vocabulary used within their presentations to provide background information or context so that audiences that had not taken the CSS 210 course could also understand the presentation.
- CSS 490 - Cybersecurity Capstone students helped write a grant proposal application for the Google Cyber Clinics Fund. Through this project, students had to consider how to convey the importance of funding a clinic at William Woods and what information would need to be shared with those assessing the application and other relevant stakeholders.
- CSS 490 online and on-ground Cybersecurity capstone students developed whitepapers that required them to research how to develop a Cybersecurity program for an organization and present it from the point of view of a company Chief Information Security Officer (CISO).

4C -

- CSS 490 - Cybersecurity Capstone students developed the plans for a malware sandboxing environment and had to analyze the development of this project from many different perspectives including budgetary requirements, technical (hardware and software) requirements, security requirements, and project purpose/benefit.

- MIS 250 - Networking on-ground students had to research Internet of Things (IoT) technologies and describe how they could be utilized and secured within a Smart City including wireless protocols, best practices, and use cases.

4D -

- CSS 210 - Introduction to Cybersecurity students evaluated Cybersecurity news and blog articles in the following in-class activity: Using some of the cybersecurity news sources/blogs in the list below, find at least 3 articles (and provide links to each of them) that discuss recent cyberattacks or events related to the evolving attack and defense methods. This activity culminated in a class discussion about the articles found, the sources they were gathered from, and the types of cyber attacks and defenses that were included in the articles.

Curriculum Map

A - Assessed
R - Reinforced
I - Introduced
M - Master

Cybersecurity Curriculum Map

	CMJ 385	CMJ 440	CSS 210	CSS 300	CSS 310	CSS 324	CSS 325	CSS 401	CSS 410	CSS 420	CSS 440
CSS.1 Discuss the impact of cybersecurity on society and organizations.			I	R	I				M, A		
CSS.2 Develop presentations and documentation to communicate technical content.	I		I, R	A	R	R	R	I			
CSS.3 Describe the process of designing a computer system.				R		R		R		R, M	R
CSS.4 Design and implement cybersecurity solutions based on a set of requirements.	I	I	I	R	I	I	I	A	A, M	R, M	R, M
CSS.5 Identify and compare computer networks and architectures.				R		R	R		R	R, M	
CSS.6 Communicate computer security principles and their application.	I	I	I, R	R	R		R	A		R, M	R, M

	CSS 451	CSS 452	CSS 490	MIS 100	MIS 225	MIS 250	MIS 350	MIS 425	MIS 450
CSS.1 Discuss the impact of cybersecurity on society and organizations.	R	R	A, M	I					
CSS.2 Develop presentations and documentation to communicate technical content.	R	R	M, A	I	I		R		
CSS.3 Describe the process of designing a computer system.	R	R	M, A			I			I
CSS.4 Design and implement cybersecurity solutions based on a set of requirements.	R	R	M, A						
CSS.5 Identify and compare computer networks and architectures.	R	R	M, A			I		I	I
CSS.6 Communicate computer security principles and their application.	R	R	M, A		I	I	I		I

Changes to Curriculum

Are there any changes made to the curriculum map for this academic year? If so, please describe the program changes made along with the rationale for why and the impact the change should have on student learning?

As of this academic year, the CSS 210 - Introduction to Cybersecurity-Q and MIS 100 - Cloud Computing-Q courses were modified to become a part of the general education courses offered to students. Both classes are within the Inquiry and Analysis category of the GE framework and include an assignment that ensures students can identify an appropriate topic for the domain and integrate relevant evidence to make informed conclusions or judgements. These classes were identified to become part of the General Education as more students could gain exposure to the Cybersecurity discipline

and they are widely applicable to nearly all majors and career fields that students may pursue beyond graduation. Outside of this change, no other major curricular changes have been made to the program other than to ensure courses maintain updated information with the rapidly changing nature of cybersecurity/technology-based fields.

Assessment Findings

Assessment Findings for the Assessment Measure level for Cybersecurity Curriculum Map

Standard/Outcome
CSS.1 Discuss the impact of cybersecurity on society and organizations.

Assessment Measures

CSS 410				
Assessment Measure	**Criterion**	**Summary**	**Attachments of the Assessments**	**Improvement Narratives**
Direct - Case Study	Has the criterion Score 75% or higher on assignment. been met yet?			- Refine Assessment Tool: Align assessment tool across online and on-ground modalities.

CSS 490				
Assessment Measure	**Criterion**	**Summary**	**Attachments of the Assessments**	**Improvement Narratives**
Direct - Class Assignment	Has the criterion Score 75% or higher on assignment. been met yet? Met	Students successfully discussed the impact of cybersecurity on society and organizations. (Data from BrightSpace for 2 FUL Cybersecurity majors that completed the assignment).	CSS_490_Assessment_Metric.PNG	- Refine Assessment Tool: Align assessment tool across online and on-ground modalities.

Standard/Outcome
CSS.2 Develop presentations and documentation to communicate technical content.

Assessment Measures

CSS 300				
Assessment Measure	**Criterion**	**Summary**	**Attachments of the Assessments**	**Improvement Narratives**
Direct - Class Assignment	Has the criterion Score 75% or higher on assignment. been met yet? Met	Student successfully developed documentation to communicate technical content. (Data from BrightSpace for 1 FUL Cybersecurity major that	CSS_300_FUL_Fall_2023___Assessment.PNG	- Refine Assessment Tool: Align assessment tool across online and on-ground modalities.

		completed the assignment).		

CSS 490				
Assessment Measure	**Criterion**	**Summary**	**Attachments of the Assessments**	**Improvement Narratives**
Direct - Class Assignment	Has the criterion Score 75% or higher on assignment. been met yet? Met	Students successfully developed documentation to communicate technical content. (Data from BrightSpace for 2 FUL Cybersecurity majors that completed the assignment).	CSS_490_Assessment_ Metric.PNG	- Refine Assessment Tool: Align assessment tool across online and on-ground modalities.

Standard/Outcome
CSS.3 Describe the process of designing a computer system.

Assessment Measures

CSS 490				
Assessment Measure	**Criterion**	**Summary**	**Attachments of the Assessments**	**Improvement Narratives**
Direct - Class Assignment	Has the criterion Score 75% or higher on assignment. been met yet? Met	Students successfully described the process of designing a computer system. (Data from BrightSpace for 2 FUL Cybersecurity majors that completed the assignment).	CSS_490_Assessment_ Metric.PNG	- Refine Assessment Tool: Align assessment tool across online and on-ground modalities.

Standard/Outcome
CSS.4 Design and implement cybersecurity solutions based on a set of requirements.

Assessment Measures

CSS 401				
Assessment Measure	**Criterion**	**Summary**	**Attachments of the Assessments**	**Improvement Narratives**
Direct - Case Study	Has the criterion Score 75% or higher on assignment. been met yet?			- Refine Assessment Tool: Align assessment tool across online and on-ground modalities.

CSS 410				

Assessment Measure	Criterion	Summary	Attachments of the Assessments	Improvement Narratives
Direct - Case Study	Has the criterion Score 75% or higher on assignment. been met yet?			- Refine Assessment Tool: Align assessment tool across online and on-ground modalities.

CSS 490				
Assessment Measure	**Criterion**	**Summary**	**Attachments of the Assessments**	**Improvement Narratives**
Direct - Class Assignment	Has the criterion Score 75% or higher on assignment. been met yet? Met	Students successfully designed and implemented cybersecurity solutions based on a set of requirements. (Data from BrightSpace for 2 FUL Cybersecurity majors that completed the assignment).	CSS_490_Assessment_Metric.PNG	- Refine Assessment Tool: Align assessment tool across online and on-ground modalities.

Standard/Outcome
CSS.5 Identify and compare computer networks and architectures.

Assessment Measures

CSS 490				
Assessment Measure	**Criterion**	**Summary**	**Attachments of the Assessments**	**Improvement Narratives**
Direct - Class Assignment	Has the criterion Score 75% or higher on assignment. been met yet? Met	Students successfully identified and compared computer networks and architectures. (Data from BrightSpace for 2 FUL Cybersecurity majors that completed the assignment).	CSS_490_Assessment_Metric.PNG	- Refine Assessment Tool: Align assessment tool across online and on-ground modalities.

Standard/Outcome
CSS.6 Communicate computer security principles and their application.

Assessment Measures

CSS 401				
Assessment Measure	**Criterion**	**Summary**	**Attachments of the Assessments**	**Improvement Narratives**
Direct - Case Study	Has the criterion Score 75% or higher on assignment. been met yet?			- Refine Assessment Tool: Align assessment tool across online and on-ground modalities.

CSS 490				
Assessment Measure	**Criterion**	**Summary**	**Attachments of the Assessments**	**Improvement Narratives**
Direct - Class Assignment	Has the criterion Score 75% or higher on assignment. been met yet? Met	Students successfully communicated computer security principles and their application. (Data from BrightSpace for 2 FUL Cybersecurity majors that completed the assignment).	CSS_490_Assessment_ Metric.PNG	- Refine Assessment Tool: Align assessment tool across online and on-ground modalities.

Analysis of the Assessment Process

Describe your assessment process; clearly articulate how the program uses coursework and or Student Performance Review for program wide assessment. Note any changes that occurred to the process since the previous year. Discuss what activities were successful and which ones were not as helpful and why. Please include who met to discuss the changes (unless you are a program of one person) and when you met. – Include a discussion on the process for collection and analysis of program data.

Paul (online) and Nina (on-ground) discussed via email the assessment report and collected some of the Assessment Materials for this reporting period during the month of May. Paul and Nina also collaborated during the Fall semester on developing questions for the Cybersecurity Assessment Quiz that was piloted with on-ground students this year and will be implemented for online students in the next reporting period.

On-ground Cybersecurity students completed a short multiple choice and true/false assessment quiz, updated their LinkedIn accounts, and saw a short presentation about Cybersecurity resources and workspaces. This was a change from the prior year where students did not take any assessment quiz on Performance Day.

The assessment quiz incorporated questions directly related to topics covered in core Cybersecurity (CSS) courses as well as the MIS 250 - Networking course as these presented the foundational cybersecurity knowledge presented throughout the program. There is a questions bank consisting of 20 True/False Questions and 45 Multiple Choice Questions where students are randomly given 10 True/False Questions and 20 Multiple Choice Questions to complete. 16 students took this assessment quiz and all students earned a 50% or higher for correct responses. Collection and analysis of this data occurred through the Statistics tab of the BrightSpace quiz that was developed for administering this assessment and the subsequent Excel report that was produced from the user metrics.

There was consideration on how best to administer this assessment quiz for online students as they do not currently participate in the Performance Day activities with the on-ground Cybersecurity students. Adding this quiz as a component to a course such as the CSS 210 OLC - Introduction to Cybersecurity-Q course was one solution that was considered, however ensuring that students who are not Cybersecurity majors don't take the exam and alter the data was something we wanted to ensure. Looking ahead at next reporting period, implementing this same assessment quiz within the CSS 210 OLC class could be achieved by including a conditional logic question about what major the student is and only directing Cybersecurity majors to the rest of the quiz.

Additionally for the next reporting period, a major focus of the assessment process for the Cybersecurity program will be aligning the assessment evaluation tools across the on-ground and online modalities to ensure consistency of data and

reporting. This will also include discussion of any potential changes going forward such as adding another point of assessment for CSS Objective 3 within the assessment map.

Improvement Narrative List

Assessment Findings for the Assessment Measure level

Standard/Outcome	CSS.2 Develop presentations and documentation to communicate technical content.
Legend	A
Course/Event	CSS 300
Assessment Measure	Direct - Class Assignment
Assessment Findings	Met
Improvement Narrative	

Improvement Type	Summary
Refine Assessment Tool	Align assessment tool across online and on-ground modalities.

Standard/Outcome	CSS.4 Design and implement cybersecurity solutions based on a set of requirements.
Legend	A
Course/Event	CSS 401
Assessment Measure	Direct - Case Study
Assessment Findings	
Improvement Narrative	

Improvement Type	Summary
Refine Assessment Tool	Align assessment tool across online and on-ground modalities.

Standard/Outcome	CSS.6 Communicate computer security principles and their application.
Legend	A
Course/Event	CSS 401
Assessment Measure	Direct - Case Study
Assessment Findings	
Improvement Narrative	

Improvement Type	Summary
Refine Assessment Tool	Align assessment tool across online and on-ground modalities.

Standard/Outcome	CSS.1 Discuss the impact of cybersecurity on society and organizations.
Legend	A
Course/Event	CSS 410
Assessment Measure	Direct - Case Study
Assessment Findings	
Improvement Narrative	

Improvement Type	Summary
Refine Assessment Tool	Align assessment tool across online and on-ground modalities.

Standard/Outcome	CSS.4 Design and implement cybersecurity solutions based on a set of requirements.
Legend	A
Course/Event	CSS 410
Assessment Measure	Direct - Case Study
Assessment Findings	
Improvement Narrative	

Improvement Type	Summary
Refine Assessment Tool	Align assessment tool across online and on-ground modalities.

Standard/Outcome	CSS.1 Discuss the impact of cybersecurity on society and organizations.
Legend	A
Course/Event	CSS 490
Assessment Measure	Direct - Class Assignment
Assessment Findings	Met
Improvement Narrative	

Improvement Type	Summary
Refine Assessment Tool	Align assessment tool across online and on-ground modalities.

Standard/Outcome	CSS.2 Develop presentations and documentation to communicate technical content.
Legend	A
Course/Event	CSS 490
Assessment Measure	Direct - Class Assignment
Assessment Findings	Met

Improvement Narrative	

Improvement Type	Summary
Refine Assessment Tool	Align assessment tool across online and on-ground modalities.

Standard/Outcome	CSS.3 Describe the process of designing a computer system.
Legend	A
Course/Event	CSS 490
Assessment Measure	Direct - Class Assignment
Assessment Findings	Met
Improvement Narrative	

Improvement Type	Summary
Refine Assessment Tool	Align assessment tool across online and on-ground modalities.

Standard/Outcome	CSS.4 Design and implement cybersecurity solutions based on a set of requirements.
Legend	A
Course/Event	CSS 490
Assessment Measure	Direct - Class Assignment
Assessment Findings	Met
Improvement Narrative	

Improvement Type	Summary
Refine Assessment Tool	Align assessment tool across online and on-ground modalities.

Standard/Outcome	CSS.5 Identify and compare computer networks and architectures.
Legend	A
Course/Event	CSS 490
Assessment Measure	Direct - Class Assignment
Assessment Findings	Met
Improvement Narrative	

Improvement Type	Summary
Refine Assessment Tool	Align assessment tool across online and on-ground modalities.

Standard/Outcome	CSS.6 Communicate computer security principles and their application.
Legend	A
Course/Event	CSS 490
Assessment Measure	Direct - Class Assignment
Assessment Findings	Met
Improvement Narrative	

Improvement Type	Summary
Refine Assessment Tool	Align assessment tool across online and on-ground modalities.

Program Activities

Student Performance Review

Describe the department Student Performance Review activities if not already articulated. Please describe the nature of the assessments conducted as well as the process of assessment happening on these two days. Include the schedule of assessment day for your program. What does the data and outcomes tell you? What changes will you make as a result of the data? What areas are successful for the program?

On-ground Cybersecurity students completed a short multiple choice and true/false assessment quiz, updated their LinkedIn accounts, and saw a short presentation about Cybersecurity resources and workspaces.

The assessment quiz incorporated questions directly related to topics covered in core Cybersecurity (CSS) courses as well as the MIS 250 - Networking course as these presented the foundational cybersecurity knowledge presented throughout the program. There is a questions bank consisting of 20 True/False Questions and 45 Multiple Choice Questions where students are randomly given 10 True/False Questions and 20 Multiple Choice Questions to complete. 16 students took this assessment quiz and all students earned a 50% or higher for correct responses.

There was consideration on how best to administer this assessment quiz for online students as they do not currently participate in the Performance Day activities with the on-ground Cybersecurity students. Adding this quiz as a component to a course such as the CSS 210 OLC - Introduction to Cybersecurity-Q course was one solution that was considered, however ensuring that students who are not Cybersecurity majors don't take the exam and alter the data was something we wanted to ensure. Looking ahead at next reporting period, implementing this same assessment quiz within the CSS 210 OLC class could be achieved by including a conditional logic question about what major the student is and only directing Cybersecurity majors to the rest of the quiz.

Student Performance Review Schedule

Upload the program schedule for students during Performance Reviews.

Student_Performance_Day_Schedule_for_SoBT_2024.docx

Senior Showcase/Symposium

Describe program activities used to highlight Senior achievement. What benefit does the program gain from the activities? What if any assessment of students happens during this event?

Seniors Dustin Russell and Jared Stephens were selected to present their CSS 490 - Cybersecurity Capstone project (Sandbox Sentinel: Building the Ultimate Malware Playground) at the 2024 Symposium of Scholarship, Research, and Creativity Outstanding Senior Competition. The two students presented at the Symposium on Thursday, April 11th, 2024.

The MIS 425 - Enterprise Systems course developed Splunk Dashboards in small groups and presented on the topics each group chose and the visualizations developed during the morning session of the Symposium on Thursday, April 11th, 2024.

Students who participate in the Symposium gain the experience of presenting in front of a larger audience outside of just their peers and the instructor for the course in order to develop their public speaking skills and learn how to tailor their presentations to different audiences.

No assessment specific activities occurred during the Symposium or Senior Showcase this reporting period.

Tools used for Assessment
Upload rubrics or other Assessment based tools used by the program that are important to the assessment process.

Service Learning
Does the Program include projects/ course content that uses the philosophy of service learning?
Yes
No (selected)

Service Learning Component
If so, how is service learning infused in the coursework within your department? Is service or community engagement in the program mission? Describe the Service Learning Activities that your students and department engaged in this past year. How did the activities improve student learning? How did the activities benefit the community?

N/A

Co-Curriculuar and LEAD Events
Describe Co-Curricular and LEAD events sponsored by program faculty. This includes LEAD and other events meant to engage students and foster learning outside of the classroom.

Hosted/Sponsored 5 LEAD events for Cybersecurity Awareness Month:

▪ Cybersecurity Awareness Month Kickoff Party (10/9/23) - provided a brief overview of Cybersecurity program activities and played Cybersecurity themed board games.

▪ Cybersecurity Movie Night (10/10/23) - Student Project for CSS 210 – Introduction to Cybersecurity - Students watched Catch Me If You Can and completed a short survey about Cybersecurity knowledge.

▪ Benefits of Internships (Cybersecurity Edition) (10/18/23) - Two seniors in the Cybersecurity department presented about the internships they completed.

▪ Biometrics and Cybersecurity (10/24/23) - Student Project for CSS 210 – Introduction to Cybersecurity - Group of two students gave a short presentation and activity that described biometrics and its connection to Cybersecurity.

▪ Project: Cyber Shield (10/25/23) - Class Project for CSS 324 – Cybersecurity & Internet Architecture - Cybersecurity class presented a short simulation that represented the importance of cybersecurity hygiene and considering what information is shared online.

Also hosted a Cybersecurity program field trip to the STL CyberCon hosted by University of Missouri-St. Louis (UMSL). This one day conference including speakers from Google, Crowdstrike, Mastercard, a career fair, and poster presentations. (10/27/23).

Student Accomplishments
Highlight special examples of student successes in the field (academic: mentor-mentee, conference presentations, competitive internship, journal acceptance; extra-curricular: horse show championship, art exhibit). This is for any accomplishment a student achieved outside of course work or the normal expectation of student success.

Seniors Dustin Russell and Jared Stephens were selected to present their CSS 490 - Cybersecurity Capstone project (Sandbox Sentinel: Building the Ultimate Malware Playground) at the 2024 Symposium of Scholarship, Research, and Creativity Outstanding Senior Competition. The two students presented at the Symposium on Thursday, April 11th.

Jared completed a remote Cybersecurity internship with Mosse Cybersecurity Institute and Dustin completed a Cybersecurity internship with the Missouri State Highway Patrol.

Alumni Accomplishments
Please highlight special examples of any successes of recently graduated alumni (acceptance or graduation graduate school, employment or professional milestones).

Dustin Russell will be continuing his graduate studies through the MBA program plus at William Woods University.

Faculty Accomplishments
Highlight special examples of faculty success in the profession/field/content area. This is for any accomplishment of a faculty member that is research or professional in nature.

Nina McKee developed a proposal for a session for the Focus on Teaching and Technology Conference (FTTC) hosted by the University of Missouri - St. Louis (UMSL). The proposal is titled Points Scored and Leaderboards: Using Games to Increase Student Engagement and was submitted on Monday, April 29th, 2024. (Anticipated date of notification about whether it is accepted to the conference will be early June 2024).

Nina McKee completed the AIS247: AI Security Essentials for Business Leaders OnDemand course through SANS Institute and earned a certificate of completion on March 14, 2024.

Nina McKee attended the Women in Cybersecurity (WiCyS) 2024 Virtual Conference on Thursday, April 18th, 2024.

Todd Larivee (adjunct) earned the (ISC)2 Security CISSP certification.

Assessment Rubric

Clear	3.000 Exceeds	2.000 Meets	1.000 Falls Below Expectations	N/A
Mission Statement Clearly Articulated weight: 1.000	The mission statement for the program is insightful and forward thinking. It aligns with the University Mission and learning objectives showing a clear alignment between the University and the program.	✓ The mission statement for the program clearly articulated and aligned with the University mission.	The mission statement is minimal at best.	N/A
Comment:				
Reflection on Student Demographics, Retention, and Degree Completion Data weight: 1.000	✓ The program provides a detailed description on the enrollment, retention, persistence and degree completion numbers. The program provides new ideas on how to improve retention of their program students or articulates what they are currently doing to keep students in their program.	The program provides a basic reflection on enrollment, retention, persistence, and degree completion data provided.	The program does not reflect on enrollment, retention, persistence, and degree completion data in a detailed way.	N/A
Comment:				
Marketing Materials weight: 1.000	✓ The program outlines the successes and needs in regards to marketing. Detailed suggestions on how to market the program and what niche areas that are program specific would benefit the marketing strategy.	The program discussed the general marketing strategy for the program.	The program provided little to no discussion on the marketing materials or approach to how to market the program.	N/A
Comment:				
Alignment to University Objectives weight: 1.000	The program provides a detailed explanation of how program courses align to the Institutional Objectives. This explanation details specific courses, or activities that coordinate with the intent of the Institutional Objectives.	✓ The program provides a basic explanation of how program courses align to the Institutional Objectives. This explanation provides a minimal understanding of how the program is aligned to the Institutional Objectives.	The program provides little to no explanation of how program courses align to the Institutional Objectives.	N/A
Comment:				
General Education alignment clearly explained weight: 1.000	The program provides a detailed explanation of the General Education criterial and how the basic skills learned are expanded upon in the program. Details include but are not limited to: specific courses, or activities that stretch the knowledge of the specific areas.	✓ The program provides a basic explanation of the General Education curriculum and how the skills learned are expanded in program courses.	The program provides a minimal explanation of the General Education curriculum and how the skills learned are expanded in program courses.	N/A
Comment:				
NSSE Objectives weight: 1.000	✓ The program provided a detailed listing of activities and assessments used within the program that focused on the identified NSSE objectives. The activities and assessments were divided out within the curriculum and impacted different cohort groups.	The program provided a basic explanation of the activities and assessments used within the program that focused on the identified NSSE objectives.	The program provided minimal explanation of the activities and assessments used within the program that focused on the identified NSSE objectives.	N/A
Comment:				
Curriculum Map alignment and changes weight: 1.000	The curriculum map is detailed and complete. All Changs made to the curriculum map are detailed with supporting rationale for the decision..	✓ The curriculum map is complete. Changes made to the curriculum map are explained with some explanation as to why the changes were implemented.	The curriculum map is not complete and little to no explanation on curricular changes was provided.	N/A
Comment:				
Assessment Map weight: 1.000	Assessment of objectives are spread out across the curriculum with a variety of assessment measures and each program objective is assessed a minimum of twice a year.	✓ Each objective is assessed a minimum of 2 times a year or an assessment rotation is explained so that all objectives are assessed. The assessments are not concentrated in one class.	The assessment map is not complete or much of the assessment happens in only one course. Not all objectives are assessed annually, nor is a plan provided on assessment.	N/A
Comment:				

Data Driven Decision-making is explained weight: 1.000	✓ An overview of program assessment is provided with details on the specific successes and challenges from the year. A detailed review of how assessment was administered over the academic year is clearly outlined.	A basic overview of program assessment is provided with some details on the successes and challenges from the year. A basic review of how assessment was administered over the academic year is outlined.	A basic overview of program assessment is not provided with little to no discussion on the administration of assessment over the academic year.	N/A
Comment:				
Documentation provided on assessment findings weight: 1.000	The program uploads all rubric and support information to support the claims in the assessment findings along with detailed instructions on the assessment process and data analysis.	✓ The program uploads all rubric and support information to support the claims in assessment findings.	The program did not upload the data to support assessment claims in the assessment findings.	N/A
Comment:				
Analysis of Assessment weight: 1.000	The program completed assessment findings for each component identified, and provided a comprehensive summary of each assessment measure identified in the report.	✓ The program completed the assessment findings for each component and provided a summary for each assessment measure.	The program did not provide a completed assessment findings for each component, nor did they complete the summary for each measure.	N/A
Comment:				
Improvement narratives are selected with intentionality weight: 1.000	The program identified Improvement Narratives that appear to move the program forward and see the bigger picture than only the specific program curriculum options	✓ The program used the provided Improvement Narratives and selected options that made sense to the objectives and issues within the assessment.	The program did not use any improvement narratives, or the ones chosen are not aligned with assessment results.	N/A
Comment:				
Student Performance Review weight: 1.000	The program described and provided a detailed account of Student performance Review activities. Data evidence provided and detailed.	✓ The program provided the schedule and a brief description of Student Performance Review with data of the results.	The program did not provide complete explanation on Student Performance Review nor did they provide data results.	N/A
Comment:				
Senior Showcase weight: 1.000	The program had all senior students participate in Senior Showcase and provided a detailed explanation of their expectation and the presentations presented.	✓ The program described the Senior showcase activities and provided some evidence of what was presented.	Little to no content of Senior showcase was provided.	N/A
Comment:				
Co Curricular and LEAD activities weight: 1.000	The program detailed the activities of LEAD and other co-curricular programing that was provided throughout the year. They provided numerous events for students.	✓ The program provided a listing of LEAD events and activities provided.	The program provided little to no description of the Co-curricular activities provided throughout the year.	N/A
Comment:				
Faculty, alumni, and Student accomplishments weight: 1.000	✓ The program provided detail updates on successes on Students, Alumni and Faculty with added information explaining the kinds of success that were experienced.	The program provided a listing of information on Students, Alumni, and faculty accomplishments.	The program provided little to no data on students, alumni, faculty accomplishments.	N/A
Comment:				

Appendix: Supplemental Data

WILLIAM WOODS UNIVERSITY GLOBAL

Online Bachelor of Science in

Cybersecurity

THE WILLIAM WOODS DIFFERENCE

Over 150 years of academic excellence

Convenient schedules designed for busy lives

100% online field practicum

Tuition promise - no tuition increases as long as you stay continuously enrolled

Transfer-friendly curriculum

DEGREE IN DEMAND

Organizations are trying to fill a worldwide gap of 3.4 million cybersecurity workers, according to a 2022 Cybersecurity Workforce Study.

Stand on the Frontlines of Information Security

PROGRAM OVERVIEW

This program prepares students to create innovative solutions to protect information in the face of growing online threats. Students will gain a deep understanding of the field, while taking courses in areas such as cybersecurity, systems analysis, cybercrime and information warfare, encryption techniques and more.

PROGRAM ADVANTAGES

William Woods University is one of only a few institutions that offers a pathway to degree completion with an online B.S. degree in cybersecurity. This program will prepare you for demanding positions in public and private sectors overseeing, operating, or protecting critical computer systems, information, networks, infrastructures and communications networks.

We offer a unique combination of academic excellence, affordability, and flexibility. As an online student, you will enjoy the benefits of this close association through our online courses and experienced faculty.

> *The Cybersecurity program prepares students for demanding positions in public and private sectors overseeing, operating, or protecting critical computer systems, information, infrastructures, and communications networks from cyber crime, cyber fraud, and cyber espionage. William Woods' students who complete this undergraduate degree are able to effectively propose solutions to securing cyber networks and ensure online security.*
>
> *~Paul Frazier, BS, MS, CISSP, online program director*

WILLIAM WOODS UNIVERSITY GLOBAL

Online Bachelor of Science in CYBERSECURITY

ADMISSION REQUIREMENTS

» GPA of 2.0 or higher

23 years old or younger:

» High School transcripts required (or GED)

» College transcripts required (if applicable)

24 years old or older:

» College transcripts required (High School transcripts required if not transferring college credits)

TRANSFER FRIENDLY

Started your degree already? We offer all general education courses online to allow you to complete a 4-year degree — online. Whether you're already on the path to a bachelor's degree or want to build on your associate degree, William Woods University is the right place for you. Talk to an Admissions Counselor to learn more and to get a free transfer credits assessment.

TUITION AND FEES

At William Woods University, we are committed to offering a number of payment options to help you finance your education. We strive to keep the expense to our students as low as the rising costs of providing a quality college education will allow.

We guarantee no increase in tuition once a program has begun provided the student remains continuously enrolled and the modality does not change.

THE BRIDGE PROGRAM

Graduate with a master's degree one year after completing your bachelor's degree with the Graduate Bridge program at William Woods.

Accreditation details can be found online at williamwoods.edu/accredited

rev. 11/7/2023

Online Bachelor of Science in Cybersecurity Courses

This degree is comprised of 120 credit-hours, with 57 credit-hours coming from the major core courses and a capstone component.

CMJ 385 Digital Evidence and Forensic Investigations

Examine digital forensics relating to both civil and criminal investigations.

CMJ 440 Cybercrime and Information Warfare

Study the growing problems of crime, terrorism and information warfare being committed using computer technology.

CMJ 447 Information Security

Examine various ways in which individuals and corporations can secure their information.

CSS 210 Introduction to Cybersecurity

Explore varying principles of systems-level information security management that are employed to achieve secure solutions.

CSS 310 Cybersecurity Law & Ethics

Analyze laws and policies dealing with cybercrime, cyber warfare and privacy.

CSS 324 Cybersecurity & Internet Architecture

Learn study technologies, processes, and practices designed to protect networks, computers, programs, and data from attacks.

CSS 325 Cyber Attacks and Defenses

Gain insight on common cyber-attacks and the techniques for identifying, detecting and defending against cybersecurity threats.

CSS 401 Encryption Techniques

Explore the development of cryptography and cryptanalysis, as well as methods used to defeat it.

CSS 410 Social Engineering

Understand what targeted information is, and how e-mails, voice messages, or even in person visits masquerade as a legitimate, trusted source.

CSS 420 Critical Infrastructures

Examine critical infrastructures identified by the Department of Homeland Security, and explore ways to manage risk and enhance security.

CSS 440 Cloud Security

Learn what Cloud Computing storage is and how to protect information stored via the Cloud.

CSS 490 Cybersecurity Capstone

Integrate learning experiences acquired throughout the BS in Cybersecurity program, while evaluating current and future topics relevant to this major.

MIS 100 Cloud Computing

Analyze the theory of online business, simulations and other pedagogical implications while considering the different implications of Web 2.0 in a business sense.

MIS 225 Database Management Systems

Develop application programs in the database environment including models of data, file organization, and data structure.

MIS 250 Networking

Explore the features of centralized, decentralized, and distributed systems with emphasis placed on LAN (Local Area Network) technologies.

MIS 350 Project Management

Examine knowledge sets, skills, and tools of project management and how project management contributes to strategic goals of an organization.

MIS 425 Enterprise Systems

Analyze the managerial applications of Internet technology for a successful Web-based competitive organization.

MIS 450 Systems Analysis

Study the methods for structured analysis and design of Information Systems including data definition, flow charting, data flows and more.

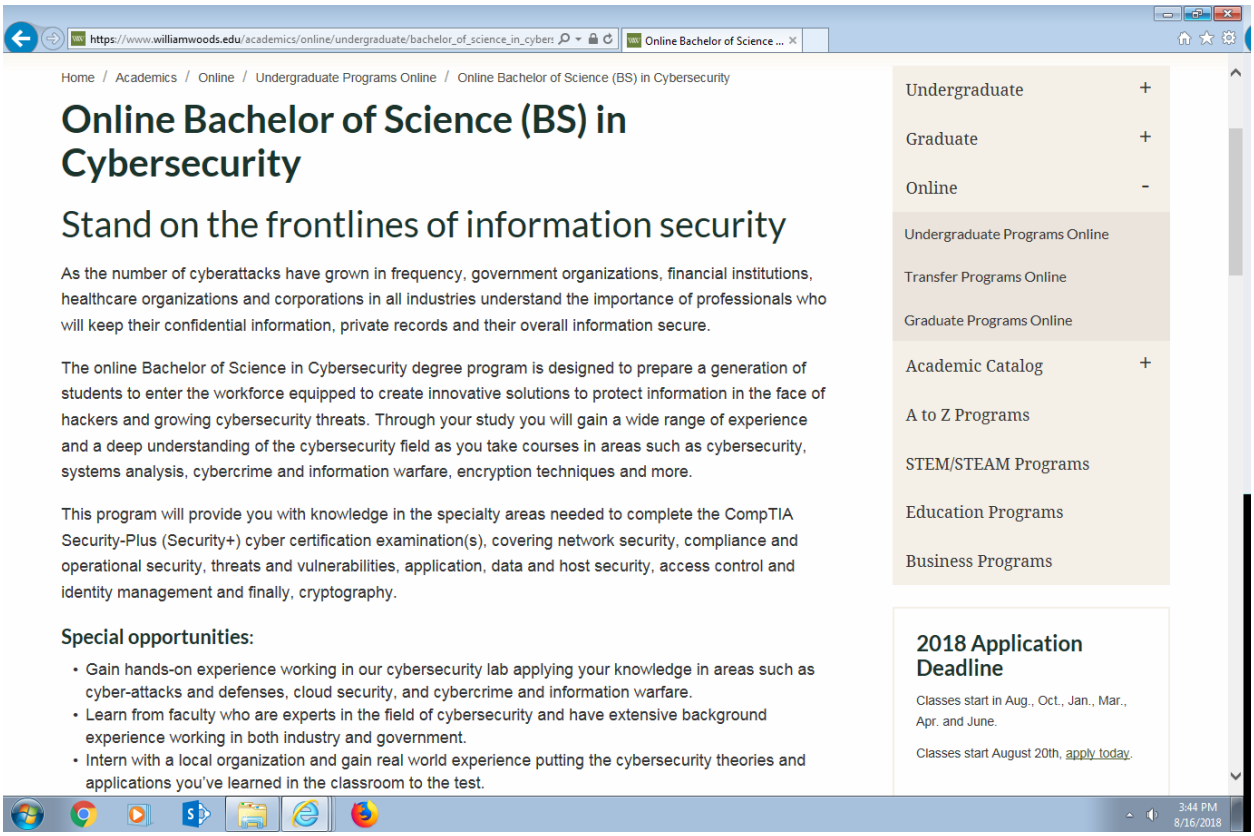
Required Electives

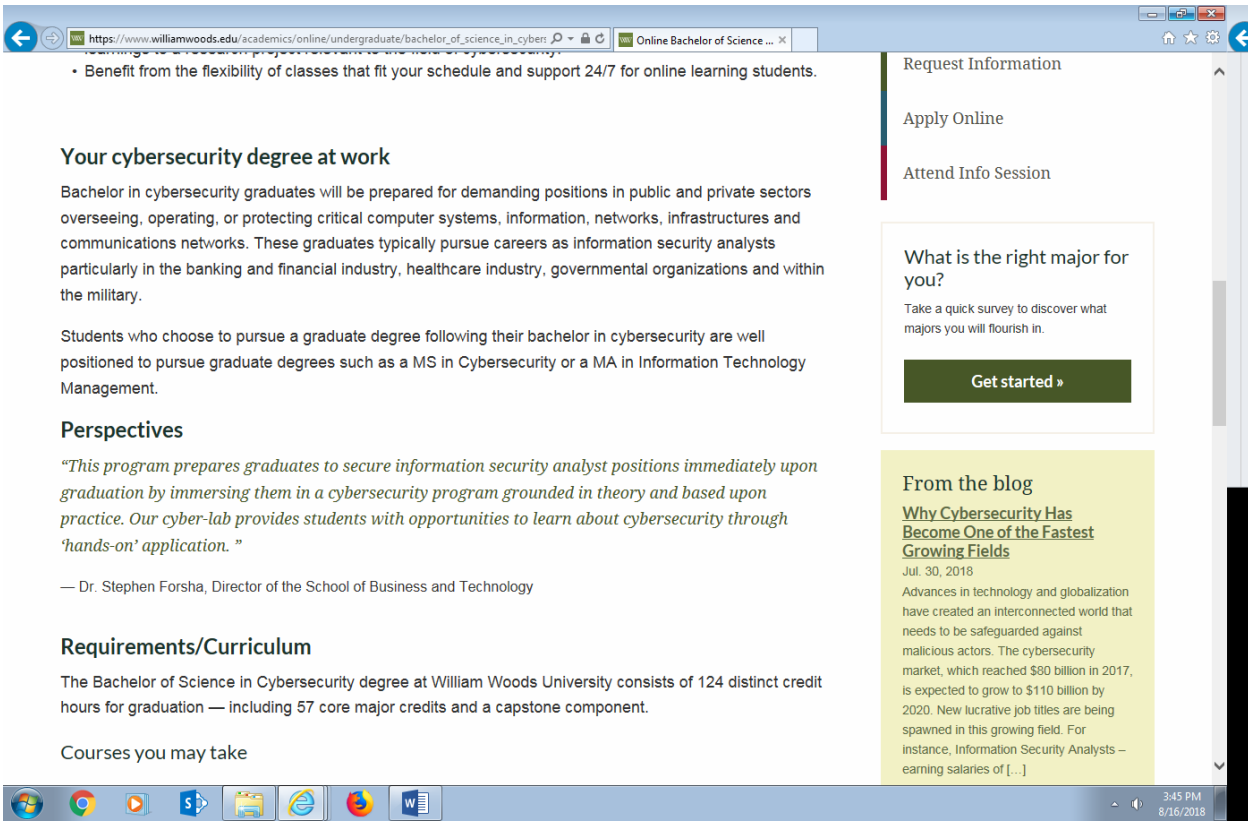
Independent Study/Internship 3.00 Credits

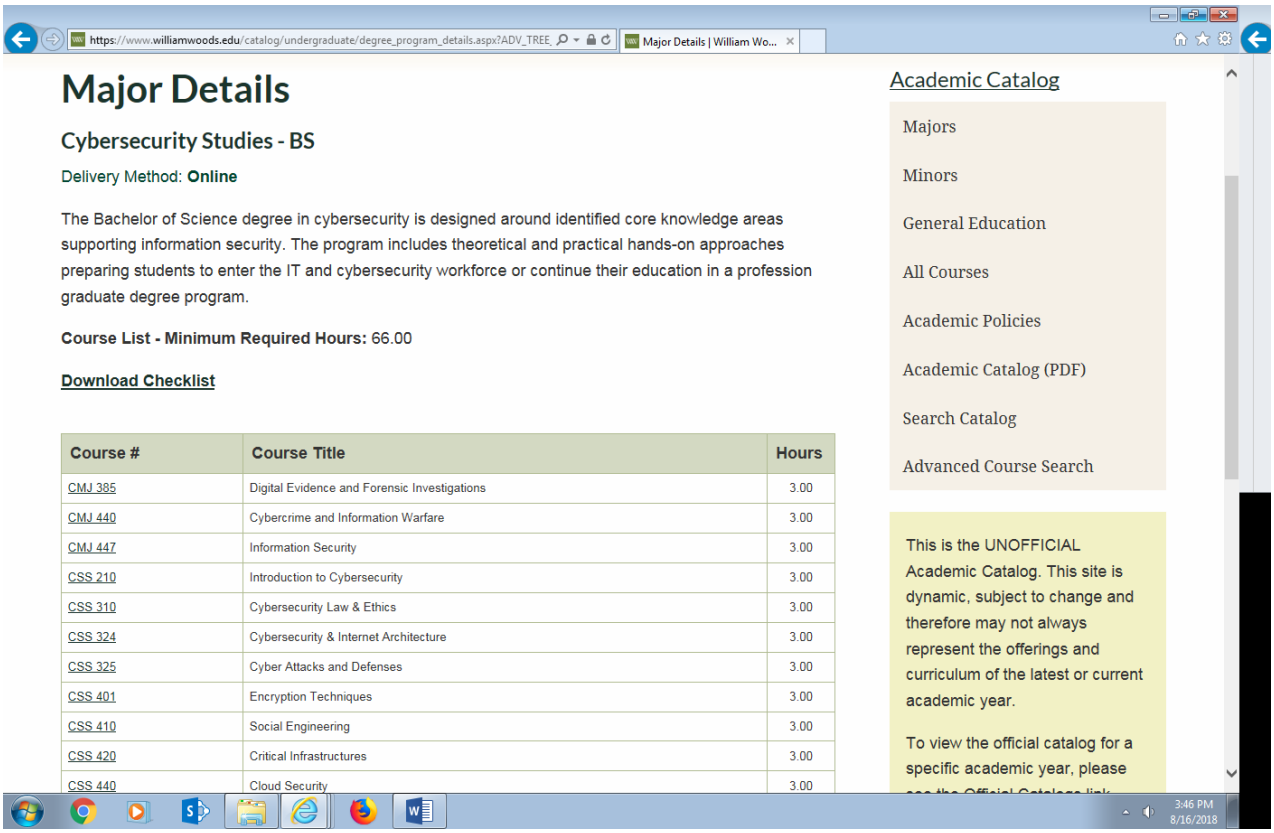
You may choose one of three course options to fulfill the 3 credit requirement.

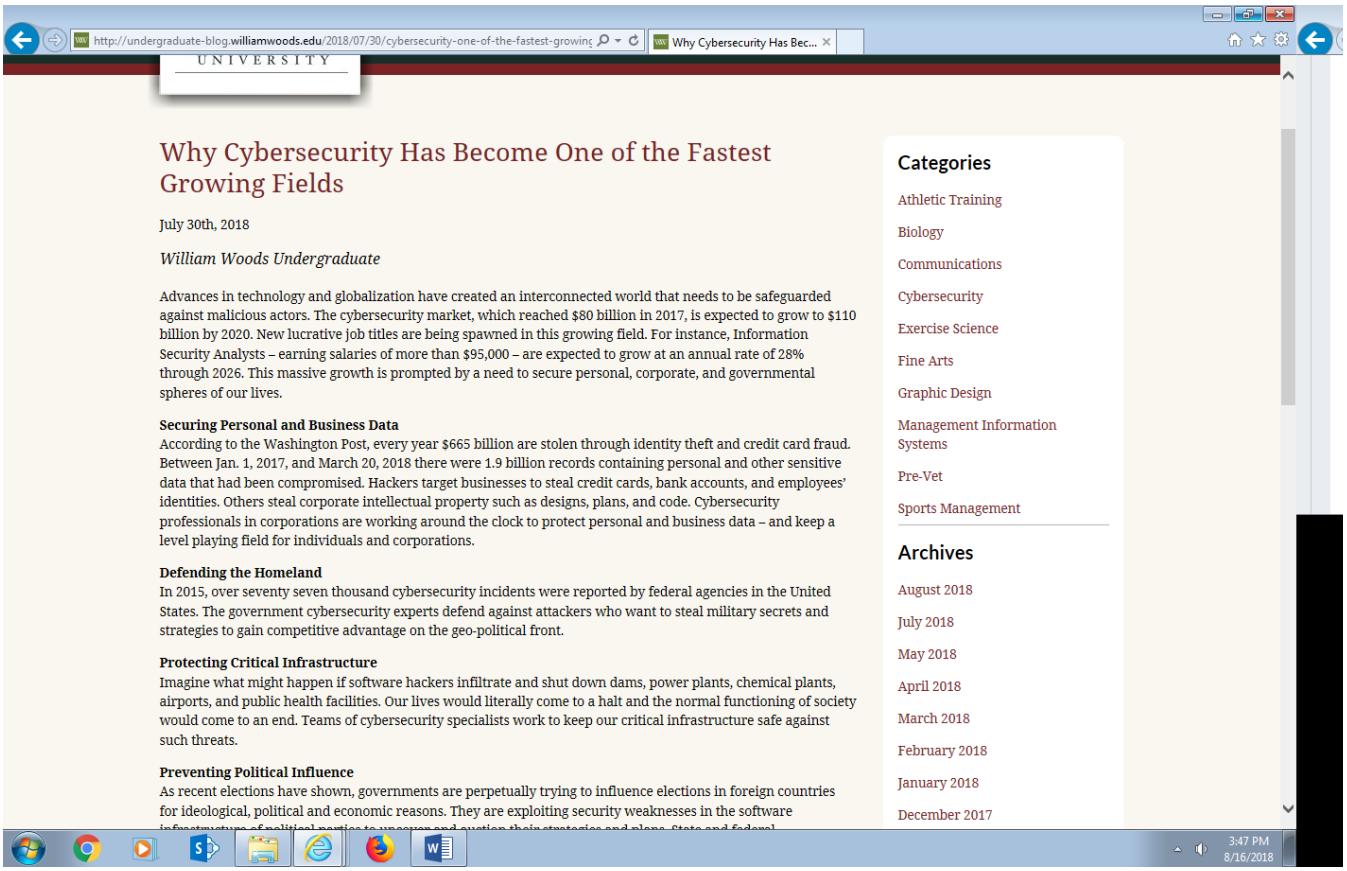
Additional Required Electives 9.00 Credits

You may choose three of 16 course options to fulfill the 9 credit requirement.


https://www.williamwoods.edu/academics/online/undergraduate/bachelor_of_science_in_cyber
Online Bachelor of Science ...
Home / Academics / Online / Undergraduate Programs Online / Online Bachelor of Science (BS) in Cybersecurity
Online Bachelor of Science (BS) in Cybersecurity
Stand on the frontlines of information security
As the number of cyberattacks have grown in frequency, government organizations, financial institutions, healthcare organizations and corporations in all industries understand the importance of professionals who will keep their confidential information, private records and their overall information secure.
The online Bachelor of Science in Cybersecurity degree program is designed to prepare a generation of students to enter the workforce equipped to create innovative solutions to protect information in the face of hackers and growing cybersecurity threats. Through your study you will gain a wide range of experience and a deep understanding of the cybersecurity field as you take courses in areas such as cybersecurity, systems analysis, cybercrime and information warfare, encryption techniques and more.
This program will provide you with knowledge in the specialty areas needed to complete the CompTIA Security-Plus (Security+) cyber certification examination(s), covering network security, compliance and operational security, threats and vulnerabilities, application, data and host security, access control and identity management and finally, cryptography.
Special opportunities:
• Gain hands-on experience working in our cybersecurity lab applying your knowledge in areas such as cyber-attacks and defenses, cloud security, and cybercrime and information warfare.
• Learn from faculty who are experts in the field of cybersecurity and have extensive background experience working in both industry and government.
• Intern with a local organization and gain real world experience putting the cybersecurity theories and applications you've learned in the classroom to the test.
Undergraduate +
Graduate +
Online -
Undergraduate Programs Online
Transfer Programs Online
Graduate Programs Online
Academic Catalog +
A to Z Programs
STEM/STEAM Programs
Education Programs
Business Programs
2018 Application Deadline
Classes start in Aug., Oct., Jan., Mar., Apr. and June.
Classes start August 20th, apply today.
3:44 PM
8/16/2018


https://www.williamwoods.edu/academics/online/undergraduate/bachelor_of_science_in_cyber
Online Bachelor of Science ...
• Benefit from the flexibility of classes that fit your schedule and support 24/7 for online learning students.
Your cybersecurity degree at work
Bachelor in cybersecurity graduates will be prepared for demanding positions in public and private sectors overseeing, operating, or protecting critical computer systems, information, networks, infrastructures and communications networks. These graduates typically pursue careers as information security analysts particularly in the banking and financial industry, healthcare industry, governmental organizations and within the military.
Students who choose to pursue a graduate degree following their bachelor in cybersecurity are well positioned to pursue graduate degrees such as a MS in Cybersecurity or a MA in Information Technology Management.
Perspectives
"This program prepares graduates to secure information security analyst positions immediately upon graduation by immersing them in a cybersecurity program grounded in theory and based upon practice. Our cyber-lab provides students with opportunities to learn about cybersecurity through 'hands-on' application."
— Dr. Stephen Forsha, Director of the School of Business and Technology
Requirements/Curriculum
The Bachelor of Science in Cybersecurity degree at William Woods University consists of 124 distinct credit hours for graduation — including 57 core major credits and a capstone component.
Courses you may take
Request Information
Apply Online
Attend Info Session
What is the right major for you?
Take a quick survey to discover what majors you will flourish in.
Get started »
From the blog
Why Cybersecurity Has Become One of the Fastest Growing Fields
Jul. 30, 2018
Advances in technology and globalization have created an interconnected world that needs to be safeguarded against malicious actors. The cybersecurity market, which reached $80 billion in 2017, is expected to grow to $110 billion by 2020. New lucrative job titles are being spawned in this growing field. For instance, Information Security Analysts – earning salaries of [...]
3:45 PM
8/16/2018


https://www.williamwoods.edu/catalog/undergraduate/degree_program_details.aspx?ADV_TREE_
Major Details | William Wo...
Major Details
Cybersecurity Studies - BS
Delivery Method: Online
The Bachelor of Science degree in cybersecurity is designed around identified core knowledge areas supporting information security. The program includes theoretical and practical hands-on approaches preparing students to enter the IT and cybersecurity workforce or continue their education in a profession graduate degree program.
Course List - Minimum Required Hours: 66.00
Download Checklist
Course # | Course Title | Hours
CMJ 385 | Digital Evidence and Forensic Investigations | 3.00
CMJ 440 | Cybercrime and Information Warfare | 3.00
CMJ 447 | Information Security | 3.00
CSS 210 | Introduction to Cybersecurity | 3.00
CSS 310 | Cybersecurity Law & Ethics | 3.00
CSS 324 | Cybersecurity & Internet Architecture | 3.00
CSS 325 | Cyber Attacks and Defenses | 3.00
CSS 401 | Encryption Techniques | 3.00
CSS 410 | Social Engineering | 3.00
CSS 420 | Critical Infrastructures | 3.00
CSS 440 | Cloud Security | 3.00
Academic Catalog
Majors
Minors
General Education
All Courses
Academic Policies
Academic Catalog (PDF)
Search Catalog
Advanced Course Search
This is the UNOFFICIAL Academic Catalog. This site is dynamic, subject to change and therefore may not always represent the offerings and curriculum of the latest or current academic year.
To view the official catalog for a specific academic year, please
3:46 PM
8/16/2018


http://undergraduate-blog.williamwoods.edu/2018/07/30/cybersecurity-one-of-the-fastest-growing
Why Cybersecurity Has Bec...
UNIVERSITY
Why Cybersecurity Has Become One of the Fastest Growing Fields
July 30th, 2018
William Woods Undergraduate
Advances in technology and globalization have created an interconnected world that needs to be safeguarded against malicious actors. The cybersecurity market, which reached $80 billion in 2017, is expected to grow to $110 billion by 2020. New lucrative job titles are being spawned in this growing field. For instance, Information Security Analysts – earning salaries of more than $95,000 – are expected to grow at an annual rate of 28% through 2026. This massive growth is prompted by a need to secure personal, corporate, and governmental spheres of our lives.
Securing Personal and Business Data
According to the Washington Post, every year $665 billion are stolen through identity theft and credit card fraud. Between Jan. 1, 2017, and March 20, 2018 there were 1.9 billion records containing personal and other sensitive data that had been compromised. Hackers target businesses to steal credit cards, bank accounts, and employees' identities. Others steal corporate intellectual property such as designs, plans, and code. Cybersecurity professionals in corporations are working around the clock to protect personal and business data – and keep a level playing field for individuals and corporations.
Defending the Homeland
In 2015, over seventy seven thousand cybersecurity incidents were reported by federal agencies in the United States. The government cybersecurity experts defend against attackers who want to steal military secrets and strategies to gain competitive advantage on the geo-political front.
Protecting Critical Infrastructure
Imagine what might happen if software hackers infiltrate and shut down dams, power plants, chemical plants, airports, and public health facilities. Our lives would literally come to a halt and the normal functioning of society would come to an end. Teams of cybersecurity specialists work to keep our critical infrastructure safe against such threats.
Preventing Political Influence
As recent elections have shown, governments are perpetually trying to influence elections in foreign countries for ideological, political and economic reasons. They are exploiting security weaknesses in the software
Categories
Athletic Training
Biology
Communications
Cybersecurity
Exercise Science
Fine Arts
Graphic Design
Management Information Systems
Pre-Vet
Sports Management
Archives
August 2018
July 2018
May 2018
April 2018
March 2018
February 2018
January 2018
December 2017
3:47 PM
8/16/2018

CYBERSECURITY

ONLINE BACHELOR OF SCIENCE

WILLIAM WOODS UNIVERSITY

flourish!

Secure a degree in a fast growing industry

This program includes theoretical and practical hands-on approaches preparing students to enter the IT and Cybersecurity workforce or continue their education in a professional graduate degree program; and, our cyber-lab allows student real world Cybersecurity, through 'hands-on' practice.

- Cloud Security
- Social Engineering
- Cyber Crime and Information Warfare
- Cyber Attack and Defense

The William Woods University Cybersecurity degree program prepares you to secure the most sought after IT positions immediately upon graduation. By immersing yourself into this online program that is grounded in theory and based upon practice, you will earn your bachelor's ready to enter an industry that, according to several employment reports, has grown 37% year-after-year since 2012.

This is not just a degree program! You will learn what you need in order to prepare for specialty areas associated with the CompTIA Security-Plus (Security+) examination(s).

Advantages and Benefits:

- 100% online
- Convenient 8-week courses
- Digital classroom available anywhere anytime
- Taught by professionals in the field of Cybersecurity



ONLINE COURSES

Our Cybersecurity program is fully online and affords students the opportunity to learn through our secure cyber lab.

UNIQUE OPPORTUNITIES

In the cyber program, students will be provided the opportunity to complete an internship or independent study project. The program will offer courses through a secure Cybersecurity lab where students will be able to apply their knowledge in areas such as cyber-attacks and defenses, cloud security, cybercrime and information warfare.

TRANSFER CREDITS

William Woods University is a transfer-friendly institution. Students who maximize transfer of credits may be able to complete the Cybersecurity program in 2 years.

CAREER OPPORTUNITIES

- Computer Systems Analyst
- Computer System Administrator
- Chief Information Security Officer
- Incident Responder
- Information Systems Manager
- Information Security Analyst
- Security Consultant
- and many more

"What is exciting about this program is the opportunity to bring Cybersecurity education to Mid-Missouri and to be able to reach students 'where they are' through our online program. Our graduates will fill an urgent need for highly-skilled cyber and information security professionals in private, military and governmental agencies."

~Stephen Forsha, Director of the School of Business and Technology

Cybersecurity Has Become One of the Fastest Growing Fields

Advances in technology and globalization have created an interconnected world that needs to be safeguarded against malicious actors. A 2018 Cybersecurity Market Report predicts cumulative spending on cybersecurity products will exceed $1 trillion over the next five years. New, lucrative job titles are being spawned in this growing field. For instance, Information Security Analysts – earning salaries of more than $95,000 – are expected to grow at an annual rate of 28% through 2026. This massive growth is prompted by a need to secure the personal, corporate, and governmental spheres of our lives.

CYBERSECURITY

WILLIAM WOODS UNIVERSITY

WILLIAM WOODS UNIVERSITY

flourish!

Learn by Doing

This program includes theoretical and practical hands-on approaches preparing students to enter the IT and cybersecurity workforce or continue their education in a profession graduate degree program. The creation of a cyber-lab in support of this program will provide students with opportunities to learn about cybersecurity through 'hands-on' practice.

Cloud Security

Social Engineering

Cyber Crime and Information Warfare

Cyber Attack and Defense

This program prepares graduates to secure information security positions immediately upon graduation by immersing them in a cybersecurity program grounded in theory and based upon practice. This experience will prepare students in specialty areas associated with the CompTIA Security-Plus (Security+) examination(s). This will provide a bachelors level education that prepares students for the cyber certification examination covering Network Security, Compliance and Operational Security, Threats & Vulnerabilities, Application, Data and Host Security, Access Control & Identity Management and finally, Cryptography.

Advantages and Banefits:

- 100% online
- Convenient 8-week courses
- Digital classroom available anywhere anytime
- Taught by professionals in the field of Cybersecurity



ONLINE COURSES

Our Cybersecurity program is fully online and affords students the opportunity to learn through our secure cyber lab.

UNIQUE OPPORTUNITIES

In the cyber program, students will be provided the opportunity to complete an internship or independent study project. The program will offer courses through a secure cybersecurity lab where students will be able to apply their knowledge in areas such as cyber-attacks and defenses, cloud security, and cybercrime and information warfare.

TRANSFER CREDITS

William Woods University is a transfer-friendly institution. Students who maximize transfer of credits may be able to complete the Cybersecurity program in 2 years.

CAREER OPPORTUNITIES

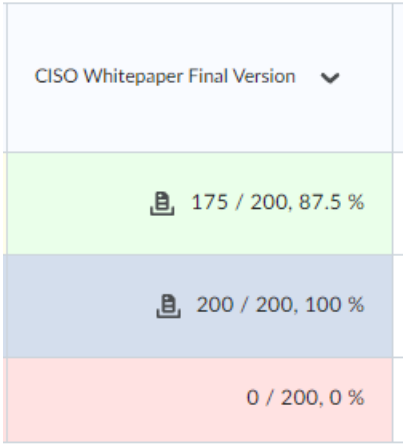
- Computer Systems Analyst
- Computer System Administrator
- Chief Information Security Officer
- Incident Responder
- Information Systems Manager
- Information Security Analyst
- Security Consultant
- and many more

"What is exciting about this program is the opportunity to bring cybersecurity education to Mid-Missouri and be able to reach students 'where they are' through our online program. Our graduates will fill an urgent need of for highly skills cyber and information security professionals in private, military and governmental agencies."

~Stephen Forsha, Director of the School of Business and Technology

	9:00 am to 11:00 am Activities		
9:00 AM 9:30 AM 10:00 AM 10:30 AM 11:00 AM	CLA Test BUR 205 (Seniors who began as WWU Freshmen) Facilitator: Carrie McCray	Internal Business/Accounting Exam BUR 206 and BUR 109 - Overflow in Burton 105 (All BUS and ACC Sophomores and Juniors) Proctors: Roman Sivkov, Jesscia Manion, David Forster, Doug Sanders	Mock Interviews + Resume Reviews BUR 101, BUR 103, BUR 203 - Think Tank Priority to Seniors and Juniors Facilitator: Scott Zimmerman and 2 Guest Interviewers (30 MIN Appointment Slots)
11:30 AM 12:00 PM 12:30 PM	LUNCH (11:30 am-1:00pm) Domino's Pizza and Water in Burton Lobby (Burton 100 and Burton 101 Overflow Lunch Seating)		
	1:00 pm to 3:00 pm Activities		
1:00 PM 1:30 PM 2:00 PM 2:30 PM 3:00 PM	Cybersecurity Assessment Quiz and Additional Activities BUR 105 (All Cybersecurity Majors) Facilitator: Nina McKee	Peregrine Exam BUR 206 and BUR 109 (All BUS and ACC Freshmen) Proctors: Roman Sivkov, Jessica Manion, David Forster	Mock Interviews + Resume Reviews BUR 101, BUR 103, BUR 203 - Think Tank Priority to Seniors and then Juniors Facilitator: Scott Zimmerman and 2 Guest Interviewers (30 MIN Appointment Slots)

Final Penetration Testing Checklist & Videos	
	150 / 150, 100 %


CISO Whitepaper Final Version
175 / 200, 87.5 %
200 / 200, 100 %
0 / 200, 0 %