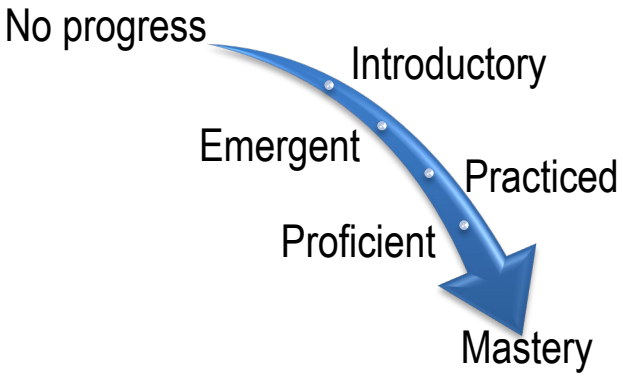
PURDUE GLOBAL
UNIVERSITY

Bachelor of Science in Cybersecurity



At Purdue University Global, we employ a method called **Course-Level Assessment**, or CLA, to determine student mastery of Course Outcomes. Through CLA, we measure how well students gain the skills, knowledge, abilities, and behaviors that employers expect of program graduates. A series of courses prepares students for employment by providing preparation, practice, and opportunities to show mastery of these program outcomes. Each course is developed around a number of learning goals, known as course outcomes, which support a student's growing mastery of program level outcomes. Faculty members assess each student's mastery of each course outcome through Course Level Assessments.

Program Measure for *Standard of Success*:

- 80% or more of students attempting the outcome will perform at the **Practiced** level or greater in **100/200** level courses
- 80% or more of students attempting the outcome will perform at the **Proficient** level or greater in **300/400** level courses.

Program Outcome	Course# / Measurement		Assessment/ Evaluation Results: % of students at or greater than Standard	Meets Criteria Yes/No
BSCYS 1: Technology Skills: Analyze a complex computing problem to apply principles of computing and other relevant disciplines to identify solutions.	IN203	Examine virtualization and container technologies.	95%	Yes
		Analyze network services.	95%	Yes
		Examine Active Directory features.	96%	Yes
		Assess endpoint protection and vulnerability management in the Windows environment.	93%	Yes
	IT262	Interpret network and reconnaissance results.	94%	Yes
	IT273	Evaluate network media types, virtualization, and network storage technologies.	98%	Yes
		Analyze policies, best practice, appropriate documentation, and diagrams to manage the network.	97%	Yes

Program Outcome	Course# / Measurement		Assessment/ Evaluation Results: % of students at or greater than Standard	Meets Criteria Yes/No
		Analyze Wide Area Networks, wireless technologies, common network attacks, and techniques for hardening network devices.	97%	Yes
	IT275	Create user and group accounts within Linux.	100%	Yes
		Configure security within the Linux operating system.	95%	Yes
	IT286	Examine the process of risk assessment and network monitoring.	92%	Yes
		Investigate device and infrastructure security, access control, authentication, and authorization.	99%	Yes
		Explain the protection of wireless networks and cloud services, and the hardening of hosts and applications.	90%	Yes
	IT390	Compare intrusion detection systems.	97%	Yes
		Analyze the security threat spectrum.	93%	Yes
		Differentiate incident response strategies.	95%	Yes
	IT395	Formulate organizational cyberthreat mitigation procedures.	89%	Yes
		Develop an ethical hacking plan to test an organization's cybersecurity posture.	88%	Yes
	IT411	Examine digital forensic concepts and techniques.	85%	Yes
		Plan appropriate methods to secure digital evidence.	89%	Yes
		Apply various types of forensic analysis tools for data recovery to forensic scenarios.	86%	Yes
		Prepare audits and investigations of electronic computing devices.	92%	Yes
		Analyze forensic data from computers to investigate security breaches.	97%	Yes

Program Outcome	Course# / Measurement		Assessment/ Evaluation Results: % of students at or greater than Standard	Meets Criteria Yes/No
		Investigate current practices and trends in digital and network forensics.	83%	Yes
	IT479	Technology Skills: Analyze a complex computing problem to apply principles of computing and other relevant disciplines to identify solutions.	98%	Yes
	IT484	Create security operations and administration procedures related to data privacy and cybersecurity policy.	95%	Yes
		Evaluate risk management and compliance in regard to cybersecurity policy and industry standards.	93%	Yes
		Evaluate cryptology, network, and communications technology used to protect private information from public disclosure and supported by cybersecurity policies.	95%	Yes
	IT497	Technology Skills: Analyze a complex computing problem to apply principles of computing and other relevant disciplines to identify solutions.	99%	Yes
BSCYS 2: System Specifications: Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.	IN203	Implement Windows servers in host and compute environments.	98%	Yes
	IT273	Analyze networking concepts, such as ports and protocols; IPv4 and IPv6 addressing; and routing and switching concepts.	97%	Yes
		Evaluate network media types, virtualization, and network storage technologies.	98%	Yes
		Analyze policies, best practice, appropriate documentation, and diagrams to manage the network.	97%	Yes
	IT275	Use the command line and the Linux software packaging system.	97%	Yes
		Configure the key features of the Linux operating system.	98%	Yes
		Modify the files in Linux.	99%	Yes

Program Outcome	Course# / Measurement		Assessment/ Evaluation Results: % of students at or greater than Standard	Meets Criteria Yes/No
	IT286	Investigate device and infrastructure security, access control, authentication, and authorization.	99%	Yes
	IT374	Configure a Linux installation.	99%	Yes
		Illustrate the information gathering process for a target environment.	98%	Yes
		Illustrate the vulnerability assessment process.	96%	Yes
		Analyze network and web exploitation.	96%	Yes
		Analyze privilege escalation and system exploitation.	99%	Yes
		Analyze wireless exploitation.	94%	Yes
	IT390	Demonstrate the ability to install and examine intrusion detection system tools.	96%	Yes
	IT479	System Specifications: Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.	100%	Yes
	IT484	Evaluate access controls and security technologies supported by cybersecurity policies used to protect network resources and ensure data availability.	95%	Yes
		Create an incident response plan, integrated with cybersecurity policy, which assists with organizational recovery.	92%	Yes
		Evaluate cryptology, network, and communications technology used to protect private information from public disclosure and supported by cybersecurity policies.	95%	Yes
		Evaluate organizational system and application security procedures related to cybersecurity policies and industry standards.	91%	Yes
	IT497	System Specifications: Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.	99%	Yes
	MM212	Analyze rational and radical expressions.	93%	Yes
BSCYS 3: Professional	CS212	Identify elements of professional presence within your field of study.	97%	Yes
		Apply techniques for presenting professionalism through social media.	99%	Yes

Program Outcome	Course# / Measurement		Assessment/ Evaluation Results: % of students at or greater than Standard	Meets Criteria Yes/No
Communication: Communicate effectively in a variety of professional contexts.		Demonstrate oral communication skills for promoting a professional image.	92%	Yes
	IN206	Prepare an IP scheme for a network using IPv6.	100%	Yes
		Explore advanced network routing and switching concepts including security.	100%	Yes
		Prepare for network security and cloud access.	100%	Yes
	IT273	Analyze policies, best practice, appropriate documentation, and diagrams to manage the network.	97%	Yes
	IT390	Interpret various security analytic measures.	91%	Yes
	IT400	Develop critical thinking methods addressing cybersecurity ethics.	87%	Yes
		Explain ethical concerns relating to privacy and confidentiality involving information technology.	90%	Yes
		Examine relevant ethical issues that proliferate the use of information technology.	92%	Yes
		Discuss laws and regulations involving ethical behavior of individuals and organizations using information technology.	86%	Yes
	IT411	Prepare audits and investigations of electronic computing devices.	92%	Yes
	IT479	Professional Communication: Communicate effectively in a variety of professional contexts.	98%	Yes
	IT497	Professional Communication: Communicate effectively in a variety of professional contexts.	96%	Yes
	CS212	Identify elements of professional presence within your field of study.	97%	Yes

Program Outcome	Course# / Measurement		Assessment/ Evaluation Results: % of students at or greater than Standard	Meets Criteria Yes/No
BSCYS 4: Professional Development: Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.		Apply logical reasoning to address issues in professionalism.	91%	Yes
	IT104	Examine the field of cybersecurity, including career opportunities and pathways to cybersecurity certifications.	97%	Yes
		Discuss the role of security assessments.	97%	Yes
		Explain current cybersecurity threats and the future of cybersecurity.	95%	Yes
	IT262	Describe steps and techniques to perform enumeration, scanning, and packet capture.	97%	Yes
		Explain encryption and social engineering attacks.	93%	Yes
	IT390	Differentiate incident response strategies.	95%	Yes
	IT395	Prepare wireless network attacks.	88%	Yes
	IT400	Explore the relevance of ethical issues that involve use of information technology.	89%	Yes
		Evaluate a broad array of topics including privacy, free speech, information security, and law.	88%	Yes
		Develop critical thinking methods addressing cybersecurity ethics.	87%	Yes
		Examine relevant ethical issues that proliferate the use of information technology.	92%	Yes
		Discuss laws and regulations involving ethical behavior of individuals and organizations using information technology.	86%	Yes
	IT411	Analyze forensic data from computers to investigate security breaches.	97%	Yes
	IT479	Professional Development: Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.	100%	Yes
	IT484	Evaluate access controls and security technologies supported by cybersecurity policies used to protect network resources and ensure data availability.	95%	Yes
		Create security operations and administration procedures related to data privacy and cybersecurity policy.	95%	Yes
		Create an incident response plan, integrated with cybersecurity policy, which assists with organizational recovery.	92%	Yes

Program Outcome	Course# / Measurement		Assessment/ Evaluation Results: % of students at or greater than Standard	Meets Criteria Yes/No
	IT497	Professional Development: Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.	98%	Yes
	MM207	Examine data appropriately.	91%	Yes
		Apply probability to real-world problems.	85%	Yes
BSCYS 5: Team Management: Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.	CS212	Identify effective strategies for promoting professionalism in teams.	92%	Yes
	IT104	Differentiate the roles of internal and external security controls.	96%	Yes
		Identify operations security and personnel cybersecurity issues.	97%	Yes
	IT244	Analyze user-defined functions and classes in Python.	98%	Yes
	IT262	Interpret network and reconnaissance results.	94%	Yes
	IT273	Analyze networking concepts, such as ports and protocols; IPv4 and IPv6 addressing; and routing and switching concepts.	97%	Yes
	IT286	Examine the process of risk assessment and network monitoring.	92%	Yes
	IT390	Discuss intrusion detection and incident response principles and concepts.	92%	Yes
		Compare intrusion detection systems.	97%	Yes
	IT395	Formulate organizational cyberthreat mitigation procedures.	89%	Yes
	IT411	Examine digital forensic concepts and techniques.	85%	Yes
		Analyze forensic data from computers to investigate security breaches.	97%	Yes
		Investigate current practices and trends in digital and network forensics.	83%	Yes
	IT479	Team Management: Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.	100%	Yes
	IT484	Evaluate access controls and security technologies supported by cybersecurity policies used to protect network resources and ensure data availability.	95%	Yes
		Create security operations and administration procedures related to data privacy and cybersecurity policy.	95%	Yes
		Create an incident response plan, integrated with cybersecurity policy, which assists with organizational recovery.	92%	Yes
	IT497	Team Management: Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.	95%	Yes

Program Outcome	Course# / Measurement		Assessment/ Evaluation Results: % of students at or greater than Standard	Meets Criteria Yes/No
BSCYS 6: Security Analysis: Apply security principles and practices to maintain operations in the presence of risks and threats.	IN203	Implement Windows servers in host and compute environments.	98%	Yes
	IT262	Describe steps and techniques to perform enumeration, scanning, and packet capture.	97%	Yes
	IT273	Analyze networking concepts, such as ports and protocols; IPv4 and IPv6 addressing; and routing and switching concepts.	97%	Yes
	IT286	Investigate device and infrastructure security, access control, authentication, and authorization.	99%	Yes
	IT374	Illustrate the information gathering process for a target environment.	98%	Yes
		Illustrate the vulnerability assessment process.	96%	Yes
		Analyze network and web exploitation.	96%	Yes
		Analyze privilege escalation and system exploitation.	99%	Yes
		Analyze wireless exploitation.	94%	Yes
	IT390	Analyze the security threat spectrum.	93%	Yes
		Demonstrate the ability to install and examine intrusion detection system tools.	96%	Yes
		Interpret various security analytic measures.	91%	Yes
		Differentiate incident response strategies.	95%	Yes
	IT395	Develop an ethical hacking plan to test an organization's cybersecurity posture.	88%	Yes
	IT411	Plan appropriate methods to secure digital evidence.	89%	Yes
		Apply various types of forensic analysis tools for data recovery to forensic scenarios.	86%	Yes
		Prepare audits and investigations of electronic computing devices.	92%	Yes
	IT479	Security Analysis: Apply security principles and practices to maintain operations in the presence of risks and threats.	98%	Yes
	IT497	Security Analysis: Apply security principles and practices to maintain operations in the presence of risks and threats.	94%	Yes

The CLA data was collected between 7/1/2020 through 6/30/2022.