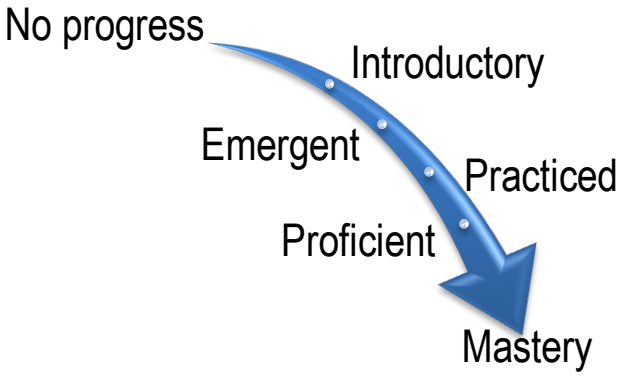
PURDUE GLOBAL UNIVERSITY

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.

BSCYS 1—Technology Skills: Analyze a complex computing problem to apply principles of computing and other relevant disciplines to identify solutions.

Course #	Measurement	Assessment/Evaluation Results: % of students at or greater than Standard	Meets Criteria
CM241	Apply fundamental technical communication skills to practice-based situations.	70%	No
CM241	Present information using digital media tools for defined audiences.	82%	Yes
IT273	Differentiate between the various types of network media, TCP/IP core protocols, and IPv4 addressing schemes typically used in a networked environment.	92%	Yes
IT273	Analyze LAN switching methods and related devices used for data transmission.	98%	Yes
IT273	Analyze wide area networks and wireless technologies used in organizational or individual computing.	95%	Yes
IT275	Create user and group accounts within Linux.	96%	Yes
IT275	Configure security within the Linux operating system.	100%	Yes

Course #	Measurement	Assessment/Evaluation Results: % of students at or greater than Standard	Meets Criteria
IT279	Identify network attacks and mitigation responses.	99%	Yes
IT283	Examine the TCP/IP networking model, IPv4 and IPv6 addressing, and basic IP packet structures.	96%	Yes
IT283	Analyze the protocols that operate at the lower layers of the TCP/IP model.	97%	Yes
IT283	Analyze IPv6 Neighbor Discovery, and addressing and name resolution on IP networks.	96%	Yes
IT283	Examine TCP/IP Transport Layer Protocols.	99%	Yes
IT283	Differentiate between IPv4 and IPv6 regarding deployment, benefits, and IP security.	98%	Yes
IT316	Analyze the processes involved in computer forensics.	94%	Yes
IT316	Examine various data acquisition methods.	82%	Yes
IT316	Compare current computer forensic tools.	94%	Yes
IT331	Describe how networking skills can improve project success.	93%	Yes
IT331	Analyze the functions of key components in information technology Infrastructure.	82%	Yes
IT331	Plan an effective IT infrastructure based on the needs of an organization.	86%	Yes
IT331	Evaluate Wide Area Network (WAN) technologies.	84%	Yes
IT374	Analyze network and web exploitation.	92%	Yes
IT374	Analyze privilege escalation and system exploitation.	97%	Yes
IT374	Analyze wireless exploitation.	98%	Yes
IT388	Explain network routing and switching concepts.	85%	Yes
IT388	Investigate network routing protocols to meet business requirements.	90%	Yes
IT388	Design VLANs based on specific situations.	88%	Yes
IT390	Compare intrusion detection systems.	92%	Yes
IT390	Analyze the security threat spectrum.	98%	Yes
IT390	Differentiate incident response strategies.	95%	Yes
IT395	Formulate organizational cyberthreat mitigation procedures.	99%	Yes
IT395	Develop an ethical hacking plan to test an organization’s cybersecurity posture.	100%	Yes
IT410	Discriminate assessment and test strategies.	93%	Yes
IT410	Analyze security control testing.	93%	Yes
IT411	Examine digital forensic concepts and techniques.	96%	Yes

Course #	Measurement	Assessment/Evaluation Results: % of students at or greater than Standard	Meets Criteria
IT411	Plan appropriate methods to secure digital evidence.	83%	Yes
IT411	Apply various types of forensic analysis tools for data recovery to forensic scenarios.	91%	Yes
IT411	Prepare audits and investigations of electronic computing devices.	92%	Yes
IT411	Analyze forensic data from computers to investigate security breaches.	96%	Yes
IT411	Investigate current practices and trends in digital and network forensics.	86%	Yes
IT479	Analyze a complex computing problem to apply principles of computing and other relevant disciplines to identify solutions.	100%	Yes
IT484	Create security operations and administration procedures related to data privacy and cybersecurity policy.	95%	Yes
IT484	Evaluate risk management and compliance in regard to cybersecurity policy and industry standards.	91%	Yes
IT484	Evaluate cryptology, network, and communications technology used to protect private information from public disclosure and supported by cybersecurity policies.	94%	Yes
IT497	Analyze a complex computing problem to apply principles of computing and other relevant disciplines to identify solutions.	95%	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.

Course #	Measurement	Assessment/ Evaluation Results: % of students at or greater than Standard	Meets Criteria
IT273	Appraise network architectures, models, topologies, and structures used in networking.	96%	Yes
IT273	Differentiate between the various types of network media, TCP/IP core protocols, and IPv4 addressing schemes typically used in a networked environment.	92%	Yes
IT273	Analyze LAN switching methods and related devices used for data transmission.	98%	Yes
IT275	Use the command line and the Linux software packaging system.	100%	Yes
IT275	Configure the key features of the Linux operating system.	81%	Yes

Course #	Measurement	Assessment/ Evaluation Results: % of students at or greater than Standard	Meets Criteria
IT275	Modify the files in Linux.	100%	Yes
IT277	Differentiate various security evaluation criteria.	99%	Yes
IT279	Apply secure design principles to network architecture.	96%	Yes
IT283	Examine the TCP/IP networking model, IPv4 and IPv6 addressing, and basic IP packet structures.	96%	Yes
IT283	Analyze IPv6 Neighbor Discovery, and addressing and name resolution on IP networks.	96%	Yes
IT286	Investigate device and infrastructure security, access control, authentication, and authorization.	98%	Yes
IT331	Analyze the functions of key components in information technology Infrastructure.	82%	Yes
IT331	Plan an effective IT infrastructure based on the needs of an organization.	86%	Yes
IT331	Evaluate Wide Area Network (WAN) technologies.	84%	Yes
IT331	Formulate a network security design.	70%	No
IT374	Configure a Linux installation.	99%	Yes
IT374	Illustrate the information gathering process for a target environment.	85%	Yes
IT374	Illustrate the vulnerability assessment process.	98%	Yes
IT388	Estimate an IP addressing scheme based on business needs.	93%	Yes
IT388	Apply router and switching configurations to meet business needs.	89%	Yes
IT388	Design VLANs based on specific situations.	88%	Yes
IT388	Prepare routing and switching proposals for management approval.	81%	Yes
IT390	Demonstrate the ability to install and examine intrusion detection system tools.	97%	Yes
IT412	Employ solutions that provide protection against system attacks.	94%	Yes
IT412	Develop information backup and data persistence procedures.	91%	Yes
IT412	Design network security policies and procedures.	98%	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.	100%	Yes

Course #	Measurement	Assessment/ Evaluation Results: % of students at or greater than Standard	Meets Criteria
IT484	Create an incident response plan, integrated with cybersecurity policy, which assists with organizational recovery.	90%	Yes
IT484	Evaluate cryptology, network, and communications technology used to protect private information from public disclosure and supported by cybersecurity policies.	94%	Yes
IT484	Evaluate organizational system and application security procedures related to cybersecurity policies and industry standards.	88%	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.	100%	Yes
MM212	Analyze rational and radical expressions.	84%	Yes

BSCYS 3—Professional Communication: Communicate effectively in a variety of professional contexts.

Course #	Measurement	Assessment/ Evaluation Results: % of students at or greater than Standard	Meets Criteria
CM241	Apply fundamental technical communication skills to practice-based situations.	70%	No
CM241	Present information using digital media tools for defined audiences.	82%	Yes
CS204	Apply communication skills for promoting a professional image.	94%	Yes
IT104	Explain current cybersecurity threats and the future of cybersecurity.	96%	Yes
IT262	Explain encryption and social engineering attacks.	99%	Yes
IT273	Appraise network architectures, models, topologies, and structures used in networking.	96%	Yes
IT273	Practice global interconnectedness as it applies to Information Technology.	83%	Yes
IT277	Explain information and asset classification.	97%	Yes
IT279	Describe security in the software development lifecycle.	97%	Yes
IT286	Explain the protection of wireless networks and cloud services, and the hardening of hosts and applications.	95%	Yes
IT316	Describe the field of computer forensics and investigations as a profession.	88%	Yes

Course #	Measurement	Assessment/ Evaluation Results: % of students at or greater than Standard	Meets Criteria
IT331	Describe how networking skills can improve project success.	93%	Yes
IT331	Practice global interconnectedness as it applies to your field of study.	88%	Yes
IT388	Explain network routing and switching concepts.	85%	Yes
IT388	Prepare routing and switching proposals for management approval.	81%	Yes
IT390	Discuss intrusion detection and incident response principles and concepts.	92%	Yes
IT400	Explain ethical concerns relating to privacy and confidentiality involving information technology.	94%	Yes
IT400	Discuss laws and regulations involving ethical behavior of individuals and organizations using information technology.	90%	Yes
IT412	Design network security policies and procedures.	98%	Yes
IT479	Professional Communication: Communicate effectively in a variety of professional contexts.	100%	Yes
IT497	Professional Communication: Communicate effectively in a variety of professional contexts.	89%	Yes

BSCYS 4—Professional Development: Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.

Course #	Measurement	Assessment/ Evaluation Results: % of students at or greater than Standard	Meets Criteria
CS204	Identify techniques for maintaining a professional presence.	99%	Yes
CS204	Apply communication skills for promoting a professional image.	94%	Yes
CS204	Assess professional goals for present and future career marketability.	96%	Yes
IT104	Examine the field of cybersecurity, including career opportunities and pathways to cybersecurity certifications.	93%	Yes
IT104	Explain current cybersecurity threats and the future of cybersecurity.	96%	Yes
IT277	Examine the three pillars of cybersecurity: Confidentiality, Integrity, Availability.	92%	Yes
IT286	Explore social engineering, security administration, disaster recovery, and incident response.	98%	Yes
IT316	Describe the field of computer forensics and investigations as a profession.	88%	Yes

Course #	Measurement	Assessment/ Evaluation Results: % of students at or greater than Standard	Meets Criteria
IT331	Analyze the functions of key components in information technology Infrastructure.	82%	Yes
IT331	Practice global interconnectedness as it applies to your field of study.	88%	Yes
IT400	Explore the relevance of ethical issues that involve use of information technology.	98%	Yes
IT400	Evaluate a broad array of topics including privacy, free speech, information security, and law.	95%	Yes
IT400	Develop critical thinking methods addressing cybersecurity ethics.	98%	Yes
IT400	Examine relevant ethical issues that proliferate the use of information technology.	98%	Yes
IT400	Discuss laws and regulations involving ethical behavior of individuals and organizations using information technology.	90%	Yes
IT410	Discriminate assessment and test strategies.	93%	Yes
IT410	Distinguish legal issues and professional ethics in information security.	89%	Yes
IT411	Investigate current practices and trends in digital and network forensics.	86%	Yes
IT412	Examine information security concepts.	96%	Yes
IT479	Professional Development: Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.	100%	Yes
IT497	Professional Development: Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.	100%	Yes
MT140	Discuss the purpose of corporate social responsibility and ethics.	91%	Yes

BSCYS 5—Team Management: Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.

Course #	Measurement	Assessment/ Evaluation Results: % of students at or greater than Standard	Meets Criteria
CM241	Apply fundamental technical communication skills to practice-based situations.	70%	No
CM241	Present information using digital media tools for defined audiences.	82%	Yes
IT104	Identify operations security and personnel cybersecurity issues.	95%	Yes
IT262	Explain encryption and social engineering attacks.	99%	Yes

Course #	Measurement	Assessment/ Evaluation Results: % of students at or greater than Standard	Meets Criteria
IT273	Practice global interconnectedness as it applies to Information Technology.	83%	Yes
IT275	Configure security within the Linux operating system.	100%	Yes
IT277	Differentiate multi-level data security controls.	98%	Yes
IT286	Explore social engineering, security administration, disaster recovery, and incident response.	98%	Yes
IT331	Plan an effective IT infrastructure based on the needs of an organization.	86%	Yes
IT374	Illustrate the information gathering process for a target environment.	85%	Yes
IT388	Prepare routing and switching proposals for management approval.	81%	Yes
IT390	Demonstrate the ability to install and examine intrusion detection system tools.	97%	Yes
IT410	Generalize key issues related to disaster recovery planning and physical security.	92%	Yes
IT410	Distinguish legal issues and professional ethics in information security.	89%	Yes
IT411	Prepare audits and investigations of electronic computing devices.	92%	Yes
IT412	Design network security policies and procedures.	98%	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
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	Create security operations and administration procedures related to data privacy and cybersecurity policy.	95%	Yes
IT484	Create an incident response plan, integrated with cybersecurity policy, which assists with organizational recovery.	90%	Yes
IT484	Evaluate organizational system and application security procedures related to cybersecurity policies and industry standards.	88%	Yes
IT497	Measure and assess risk management practices and policies for an enterprise network.	83%	Yes

BSCYS 6—Security Analysis: Apply security principles and practices to maintain operations in the presence of risks and threats.

Course #	Measurement	Assessment/ Evaluation Results: % of students at or greater than Standard	Meets Criteria
IT104	Examine the field of cybersecurity, including career opportunities and pathways to cybersecurity certifications.	93%	Yes
IT104	Discuss the role of security assessments.	95%	Yes
IT104	Differentiate the roles of internal and external security controls.	95%	Yes
IT104	Identify operations security and personnel cybersecurity issues.	95%	Yes
IT262	Interpret network and reconnaissance results.	97%	Yes
IT262	Describe steps and techniques to perform enumeration, scanning, and packet capture.	97%	Yes
IT262	Produce network and web server attacks.	98%	Yes
IT262	Produce wireless attacks and malware.	99%	Yes
IT262	Explain encryption and social engineering attacks.	99%	Yes
IT277	Examine the three pillars of cybersecurity: Confidentiality, Integrity, Availability.	92%	Yes
IT277	Differentiate multi-level data security controls.	98%	Yes
IT277	Distinguish access control, integrity, and information flow security models.	100%	Yes
IT277	Differentiate various security evaluation criteria.	99%	Yes
IT279	Examine engineering processes and secure design principles.	96%	Yes
IT279	Analyze symmetric and asymmetric cryptosystem fundamentals.	99%	Yes
IT279	Apply secure design principles to network architecture.	96%	Yes
IT279	Identify network attacks and mitigation responses.	99%	Yes
IT279	Describe security in the software development lifecycle.	97%	Yes
IT283	Differentiate between IPv4 and IPv6 regarding deployment, benefits, and IP security.	98%	Yes
IT286	Examine the process of risk assessment and network monitoring.	88%	Yes
IT286	Investigate device and infrastructure security, access control, authentication, and authorization.	98%	Yes
IT286	Explain the protection of wireless networks and cloud services, and the hardening of hosts and applications.	95%	Yes
IT286	Examine cryptography methods, vulnerabilities, threats, and malicious attacks.	98%	Yes

Course #	Measurement	Assessment/ Evaluation Results: % of students at or greater than Standard	Meets Criteria
IT286	Explore social engineering, security administration, disaster recovery, and incident response.	98%	Yes
IT316	Examine the relationship of computers and criminal behavior.	92%	Yes
IT316	Describe the field of computer forensics and investigations as a profession.	88%	Yes
IT316	Analyze the processes involved in computer forensics.	94%	Yes
IT316	Examine various data acquisition methods.	82%	Yes
IT316	Compare current computer forensic tools.	94%	Yes
IT316	Recommend techniques of data analysis and validation for high-tech investigations.	78%	No
IT374	Illustrate the information gathering process for a target environment.	85%	Yes
IT374	Illustrate the vulnerability assessment process.	98%	Yes
IT374	Analyze network and web exploitation.	92%	Yes
IT374	Analyze privilege escalation and system exploitation.	97%	Yes
IT374	Analyze wireless exploitation.	98%	Yes
IT390	Discuss intrusion detection and incident response principles and concepts.	92%	Yes
IT390	Compare intrusion detection systems.	92%	Yes
IT390	Analyze the security threat spectrum.	98%	Yes
IT390	Demonstrate the ability to install and examine intrusion detection system tools.	97%	Yes
IT390	Interpret various security analytic measures.	98%	Yes
IT390	Differentiate incident response strategies.	95%	Yes
IT395	Conduct social engineering and physical security attacks.	100%	Yes
IT395	Illustrate Trojans, malware, and cryptology attacks.	97%	Yes
IT395	Devise Web server and Web application attacks.	90%	Yes
IT395	Prepare wireless network attacks.	98%	Yes
IT395	Formulate organizational cyberthreat mitigation procedures.	99%	Yes
IT395	Develop an ethical hacking plan to test an organization’s cybersecurity posture.	100%	Yes
IT410	Analyze security control testing.	93%	Yes
IT410	Examine foundational security operations concepts.	93%	Yes
IT410	Determine incident prevention and response strategies.	88%	Yes
IT410	Generalize key issues related to disaster recovery planning and physical security.	92%	Yes

Course #	Measurement	Assessment/ Evaluation Results: % of students at or greater than Standard	Meets Criteria
IT411	Plan appropriate methods to secure digital evidence.	83%	Yes
IT411	Apply various types of forensic analysis tools for data recovery to forensic scenarios.	91%	Yes
IT411	Prepare audits and investigations of electronic computing devices.	92%	Yes
IT411	Analyze forensic data from computers to investigate security breaches.	96%	Yes
IT411	Investigate current practices and trends in digital and network forensics.	86%	Yes
IT412	Examine information security concepts.	96%	Yes
IT412	Analyze system vulnerabilities and threats.	100%	Yes
IT412	Choose data encryption techniques and confidentiality best practices.	100%	Yes
IT412	Employ solutions that provide protection against system attacks.	94%	Yes
IT412	Develop information backup and data persistence procedures.	91%	Yes
IT412	Design network security policies and procedures.	98%	Yes
IT479	Security Analysis: Apply security principles and practices to maintain operations in the presence of risks and threats.	100%	Yes
IT497	Security Analysis: Apply security principles and practices to maintain operations in the presence of risks and threats.	100%	Yes

The CLA data was collected between 7/1/2017 and 6/30/2019.