Enriching a Cybersecurity Course with a Professional Certificate

A Case Study

workcred
an affiliate of ANSI

The University of Texas System

Workcred, Inc.
1899 L Street, NW, 11th floor
Washington, DC 20036
www.workcred.org

Formed in 2014, Workcred is an affiliate of the American National Standards Institute (ANSI). Its mission is to strengthen workforce quality by improving the credentialing system, ensuring its ongoing relevance, and preparing employers, workers, educators, and governments to use it effectively. Workcred's vision is a labor market that relies on the relevance, quality, and value of workforce credentials for opportunities, growth, and development.

The University of Texas System
210 West 7th Street
Austin, TX 78701-2982
www.utsystem.edu

With 14 institutions that enroll over 256,000 students overall, The University of Texas System is the largest university system in Texas and one of the largest public university systems in the United States. UT institutions produced over 66,000 graduates last year and awarded more than one-third of the undergraduate degrees in Texas. They also educate more than one-half of the state's health care professionals and award 63 percent of the state's medical degrees annually. The combined efforts of UT-owned and affiliated hospitals and clinics resulted in nearly 10.8 million outpatient visits and more than 2.1 million hospital days in 2023. UT's $4.3 billion research enterprise is one of the nation's most innovative, ranking number one in Texas and number two in the U.S. for both total and federal research expenditures. With an operating budget of $32 billion for fiscal year 2025, UT institutions collectively employ more than 160,000 faculty, health care professionals, support staff, and students.

Suggested citation:

Workcred and the University of Texas System, *Enriching a Cybersecurity Course with a Professional Certificate: A Case Study* (Workcred, May 2025): **https://share.ansi.org/wc/Shared%20Documents/Workcred-Reports/UT-System-Case-Studies/Enriching-a-Cybersecurity-Course-with-a-Professional-Certificate.pdf.**

Table of Contents

Background

The state of Texas continues to experience strong job growth, which increases the need for employers to be able to hire workers with necessary skills upon graduation.[1] To address this challenge, The University of Texas System (UT System) launched the **Texas Credentials for the Future Initiative** in 2021 to create more opportunities for students, alumni, and incumbent workers to earn short-term credentials (i.e., professional certificates and microcredentials). Through partnerships with Coursera and Google, as well as initial grant funding from Strada Education Foundation, the UT System scaled microcredentials across their institutions to expand career opportunities, help students understand how skills learned in an academic course or program are connected to skills required by employers, and to improve post-graduate wages.[2]

Faculty members were given flexibility to implement strategies that were best suited for their academic disciplines, courses, and students. They could adopt existing professional certificates or develop their own microcredential. Faculty could also determine if a microcredential should be embedded in a course, offered as a co-curricular activity, or as a combination of the two.

This case study focuses on how two courses in the Google Professional Cybersecurity Certificate can be integrated into an academic course, and how the remaining certificate courses are mapped to an entire curriculum to create a pathway for certificate completion. This is part of a series of four case studies that highlight how faculty in different academic disciplines at three UT System institutions utilized microcredentials in their undergraduate courses.

> **"I am honored to collaborate with faculty and staff within our System to support collective efforts to improve the career readiness of our learners by providing access to industry credentials that supplement degrees to help our learners be competitive in the evolving world of work."**
>
> **– Kelvin Bentley, Ph.D., program manager, Texas Credentials for the Future, The University of Texas System**

1 "Over 26,000 Jobs Added as Texas Labor Market Continues Growth Streak," Texas Workforce Commission, April 18, 2025, **https://www.twc.texas.gov/news/over-26000-jobs-added-texas-labor-market-continues-growth-streak**.

2 "Texas Credentials for the Future," The University of Texas System, accessed February 12, 2025, **https://www.utsystem.edu/sites/texas-microcredentials**.

Determining the Focus and Rationale for Cybersecurity Microcredentials

The gap between the number of cybersecurity professionals needed by the government, private sector, and academia, and the number of people who possess the skills and competencies to fill the available jobs continues to increase. Thus, the need for cybersecurity professionals will continue to rise. The Bureau of Labor Statistics projects that the employment of cybersecurity professionals in the United States will increase by 33 percent between 2023 and 2033, which is much faster than the four percent average growth rate for all professions.[6] The gap also exists in the San Antonio, Texas metropolitan

Figure 1: UTSA Demographics

UTSA
The University of Texas at San Antonio™

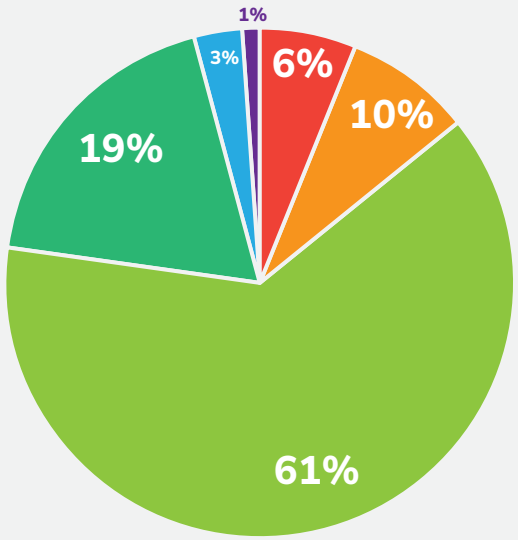
1 UTSA Circle
San Antonio, Texas 78249

University Demographics[3]

35,770 Total student enrollment

30,889 Undergraduate student enrollment

Undergraduate student demographic profile:



45% Percentage of students receiving Pell grants[4]

2,994 Total number of students enrolled in any microcredential at UTSA (July 2024)[5]

3 "Student Demographics Dashboard," UTSA Institutional Research & Analysis, Fall 2024, https://www.utsa.edu/ir/content/dashboards/student-demographics.html.

4 Rita Mitra, as submitted to case study author Karen Elzey, Workcred, October 30, 2024.

5 "New Carnegie Classification Casts Light on UTSA's Excellence in Advancing Social Mobility," UTSA Today, April 24, 2025, https://www.utsa.edu/today/2025/04/story/carnegie-classification-advancing-social-mobility.html.

6 "Occupational Outlook Handbook: Information Security Analysts," Bureau of Labor Statistics, U.S. Department of Labor, accessed April 18, 2025, https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

area, where there are only enough cybersecurity workers to fill 84 percent of the job openings.[7] And, employers state that only 28 percent of cybersecurity job applicants are well qualified for open jobs.[8] All of these challenges are leading faculty to brainstorm additional methods to ensure that students are prepared to meet the workforce needs of employers.

To better prepare students for the security workforce, Dr. Rita Mitra, professor of practice in the department of information systems and cybersecurity, The Carlos Alvarez College of Business at The University of San Antonio (UTSA), integrated a variety of industry professional certificates, certifications, and training opportunities into information systems and cybersecurity courses. Each carefully selected workforce-focused credential serves a specific purpose in the curriculum. For example, the Google Cybersecurity Professional Certificate is used to provide the needed technical and conceptual background for students who might have little or no experience with the field, while the Akamai Networking Engineering Professional Certificate is used to provide students with more practice with networking, a critical area in cybersecurity. A Cloud Support Associate or Data Analytics certificate can be offered as an alternative pathway for advanced students to learn about key adjacent topics in the field. In addition, the GitHub Copilot Certification allows students to demonstrate their competence in emerging technologies such as artificial intelligence. Students are also assigned experiential activities to obtain more real-world, hands-on cybersecurity training through platforms such as TryHackMe, HacktheBox, TryCyber, Cisco Academy, Red Hat Academy, and more.

This case study focuses on how the Google Cybersecurity Professional Certificate is integrated into the information systems and cybersecurity degree programs at UTSA, with a particular emphasis on the course, IS 1003 “Unlocking Cyber.”

7 “Cybersecurity Supply Demand Heat Map,” CyberSeek, accessed April 24, 2025, **https://www.cyberseek.org/heatmap.html**.

8 *State of Cybersecurity 2024 Report: Global Update on Workforce Efforts, Resources, and Cyberoperations* (ISACA, October 1, 2024), **https://www.isaca.org/resources/reports/state-of-cybersecurity-2024**.

Approval, Adoption, and Integration of a Cybersecurity Microcredential

Align Course Learning Objectives with the Certificate Course Content

There are several information technology (IT) and cybersecurity professional certificates and certifications in the marketplace. Yet, not all of them include content that is relevant to an undergraduate information security and cybersecurity curriculum. To determine which ones are relevant, Dr. Mitra frequently pilots and even earns credentials to review their effectiveness.

One of the credentials that was reviewed and selected by Dr. Mitra is the Google Cybersecurity Professional Certificate, which is offered through the Coursera Career Academy. There is no cost for students to earn the certificate because of a partnership among the UT System, Coursera, and Google that allows students, faculty, and staff to have free access to professional certificates offered through the Coursera Career Academy.[9] At UTSA, Dr. Claudia Arcolin, executive director of teaching and learning experiences, leads the microcredential efforts, including managing the distribution of Coursera Career Academy licenses and supporting faculty in revising their course curricula and design to effectively integrate microcredentials.

> **"Embedding microcredentials in my classes offers me with the opportunity to create customized pathways in collaboration with students based on their unique experiences. This encourages students to take a proactive approach to their own learning!"**
>
> **– Dr. Rita Mitra, professor of practice in the department of information systems and cybersecurity, The Alvarez College of Business, UTSA**

Dr. Mitra mapped the content in the Google Cybersecurity Professional Certificate to the learning outcomes in IS 1003 and the other cybersecurity core courses. In IS 1003, the first two courses in the Google certificate aligns nicely with the academic course. Figure 2 shows the cybersecurity and information systems courses at UTSA that may be mapped to the Google Cybersecurity Professional Certificate. Not all instructors include the

9 "Texas Credentials for the Future," The University of Texas System, accessed February 12, 2025, **https://www.utsystem.edu/sites/texas-microcredentials**.

Google Cybersecurity Professional Certificate courses as part of their academic course. So, if a student wants to earn the certificate on their own, they can follow the course map that shows which certificate courses are aligned with the relevant academic courses. Only the eighth course, "Put It to Work: Prepare for Cybersecurity Jobs," is not currently aligned to an academic course at UTSA.

Figure 2: Alignment between Academic Courses in the Cybersecurity and Information Systems Majors at UTSA with the Google Cybersecurity Professional Certificate

GOOGLE CYBERSECURITY PROFESSIONAL CERTIFICATE COURSES	ALIGNMENT OF CERTIFICATE COURSES TO COURSES FOR CYBERSECURITY MAJORS	ALIGNMENT OF CERTIFICATE COURSES TO COURSES FOR INFORMATION SYSTEMS MAJORS
Course 1—Foundations of Cybersecurity **Course 2—Play It Safe: Manage Security Risks**	IS 1003, Unlocking Cyber	IS 1003, Unlocking Cyber
Course 3—Connect and Protect: Networks and Network Security	IS 3413, Telecommunications and Networking	IS 3413, Telecommunications and Networking
Course 4—Tools of the Trade: Linux and SQL **Course 5—Assets, Threats, and Vulnerabilities**	IS 3033, Operating Systems and Security	IS 3063, Database Management for Information Systems
Course 6—Sound the Alarm: Detection and Response	IS 3523, Intrusion Detection and Incident Response	IS 4053, Systems Analysis and Design
Course 7—Automate Cybersecurity Tasks with Python	IS 2053, Programming I	IS 2053, Programming I
Course 8—Put It to Work: Prepare for Cybersecurity Jobs	Not aligned with any specific course, but should be completed by the end of IS 3523, Intrusion Detection and Incident Response	Not aligned with any specific course, but should be completed by the end of IS 4233, Cloud Computing

The primary audience to earn the Google certificate is undergraduate students pursing a Bachelor of Business Administration (B.B.A.) degree in cybersecurity or the online B.B.A. degree in cybersecurity, as well as those students pursing a B.B.A. in information systems and technology. Required courses that are part of academic minors in information systems, digital forensics, and cybersecurity can also be mapped to the Google Cybersecurity Professional Certificate. And, since the minor in information systems and technology is available to any student at the university, it provides more options for students to either take additional courses that are aligned with the Google Cybersecurity Professional Certificate or to pursue the certificate on their own time.

Students who enter these programs arrive from a variety of backgrounds and familiarity with technology. Some of the students are first-generation college students, some have no training in cybersecurity, others have strong

STEM backgrounds, and some students even have experience “hacking” informally or formally in their K-12 education. Integrating the first two courses of the Google Cybersecurity Professional Certificate into IS 1003 helps to establish a common baseline for all degree program students before they move on other courses in the sequence. Additionally, the students who are new to cyber gain confidence with the subject and a sense of belonging in the field. The more advanced students are given alternative Coursera Career Academy courses to complete that are customized to their background and interests.

Collaborate to Create Consensus

Because the microcredentials that are integrated into the cybersecurity curriculum counts for no more than 10 percent of the total course grade, each faculty member can include a microcredential as an enhancement to the robust curriculum that is already in place. The faculty member makes the decision about what microcredential will be used in their course in consultation with the course coordinator and the departmental programming committee. For faculty who would like guidance on strategies to incorporate third-party credentials, they can work with staff at the Division of Academic Innovation, which includes the office of teaching, learning & digital transformation at UTSA.

Design Credentials Intentionally

Dr. Mitra developed IS 1003 as an open educational resource (OER), incorporating materials that are freely accessible with open source, open access resources, or available through UTSA partnerships. Students work collaboratively within and across sections of IS 1003 using Slack, a cloud-based collaboration tool. Students must complete five “Participation Journal” activities, ten quizzes, eight labs, two courses from the Google Cybersecurity Professional Certificate, and one final exam to successfully complete the course, totaling 1000 points (see Figure 4). The two courses from the Google Cybersecurity Professional Certificate are each worth 50 points for a total of 100 points, or 10 percent of the total course grade. As outlined in Figure 3, each of those two Google certificate courses consists of four modules.

Figure 3: The First Two Courses and Corresponding Modules of the Google Cybersecurity Professional Certificate

GOOGLE CERTIFICATE COURSE MODULES	COURSE 1 – FOUNDATIONS OF CYBERSECURITY	COURSE 2 – PLAY IT SAFE: MANAGE SECURITY RISKS
Module 1	Welcome to the exciting world of cybersecurity	Security domains
Module 2	The evolution of cybersecurity	Security frameworks and controls
Module 3	Protect against threats, risks, and vulnerabilities	Introduction to cybersecurity tools
Module 4	Cybersecurity tools and programming languages	Use playbooks to respond to incidents

The modules in both courses include a variety of readings, videos, assignments, and hands-on activities.[10] Although the Google Professional Certificate courses include relevant hand-on activities, Coursera does not require students to complete the hands-on activities to earn the certificate. Therefore, the exercises and labs in the course, which are created from scratch and frequently updated, are worth 60 percent of the students' grade, and provide students with hands-on skills that they will use in real-world contexts.

Figure 4: Deliverables, Points, and Percentage of Overall Grade for IS 1003

IS 1003 COURSE DELIVERABLES	POINTS	PERCENTAGE OF OVERALL GRADE
Participation	50 points	5%
Quizzes	150 points	15%
Labs	600 points	60%
Career Academy Course	100 points	10%
Final Exam	100 points	10%
Total	1,000 points	100%

To help the students stay on track to complete the required Google certificate courses by the due dates, there is a suggested timeline, which details when students should try to complete each module. The timeline also includes the estimated time to complete each module. Students do not need to follow the timeline, but they must complete the courses by the deadlines. Students can pass Google certificate courses with a score of at least 80 percent.

Once students complete each course, they receive a certificate of completion, which they upload to Canvas, the learning management system utilized by UTSA. Students must also submit a reflection detailing how useful and interesting they found the Google Professional Cybersecurity Certificate courses taken in Coursera. Students who go on and complete the entire Google Cybersecurity Professional Certificate will receive a badge that they can use to provide external validation of the skills they have learned and to signal their knowledge, skills, and abilities to employers.

10 "Google Cybersecurity Professional Certificate," Coursera, accessed March 26, 2025, **https://www.coursera.org/professional-certificates/google-cybersecurity**.

Measurement and Success

The Division of Academic Innovation at UTSA collaborates with the office of institutional research to evaluate the impact of microcredentials on student outcomes, focusing on persistence and retention by analyzing grade distribution and the effectiveness of these credentials in promoting student success. Additionally, the division is conducting a longitudinal study to assess how microcredentials influence students' academic and career trajectories—examining whether they guide the selection of elective courses, encourage additional coursework, reinforce existing areas of study, or inspire interest in new fields.

Completion rates and DFW rates (the percentage of students receiving D or F grades or withdrawing from a course) are also collected and analyzed. In addition, Dr. Mitra conducts reviews each semester to ensure that the microcredentials used in her courses continue to meet the labor market needs. If a microcredential no longer has labor market value, it is removed. This process is especially important in the fields of information systems and cybersecurity, where knowledge and skills are rapidly evolving and labor market needs continuously change.

> **"This collaborative approach not only fosters innovation but also ensures that microcredentials are developed with student engagement and success in mind."**
>
> **– Claudia Arcolin - executive director of teaching and learning experiences, UTSA**

Lessons Learned, Challenges, and Conclusion

Require Student Reflection

As previously discussed, after submitting evidence that the students completed the first two courses of the Google Professional Cybersecurity Certificate, they submit a reflection. When submitting evidence for the first course, they answer the question, "how useful and interesting did you find this course?" Dr. Mitra uses this input to gain insights into how much students value the Google Cybersecurity Professional Certificate courses taken and to share that information as part of the reports to Coursera.

> **"This course was informative in the sense that it gave me an overview of what tools security practitioners use in their day-to-day jobs."**
>
> **– Student, IS 1003**

Provide Alternatives for Advanced Students

Providing flexibility for students is critical to address their different needs. A student who enrolls in IS 1003 may have already completed the first two courses or the entire Google Cybersecurity Professional Certificate on their own. Instead of just accepting the certificate that the students have earned and applying it to meet the course requirements, Dr. Mitra works with the students to identify another certificate that may interest them, such as the AWS Cloud Support Associate Professional Certificate or the Google Data Analytics Professional Certificate. This ensures that all students fulfill the requirements of completing a third-party certificate as part of the IS 1003 course.

Supplement the Certificate with Faculty-developed Hands-on Activities

Since students can complete the two courses of the Google Cybersecurity Professional Certificate without doing the hands-on activities, another way to measure application of knowledge and skills is needed. To that end, Dr. Mitra develops and includes hands-on labs that are the core components of the IS 1003 experience. The Google certificate offers some contextualization for these labs as background knowledge that may be assumed. In the future, Dr. Mitra is considering requiring select Google cybersecurity labs to enrich the course further.

Promote Employer Recognition

Many of the third-party credentials in information systems and cybersecurity are developed by employers and industry associations, so there is an implied value in the labor market. Despite this, it might still be beneficial to identify existing mechanisms or create new ways to gather and incorporate feedback from alumni and employers that can be used to bolster the value proposition when aligning third-party credentials and microcredentials with academic courses. This could include conducting focus groups or issuing a survey to employers and alumni to gather feedback about how the credential is valued in the hiring process. Additionally, a continuous feedback process can be established to reconvene the focus groups or reissue the survey periodically and use the insights gleaned to determine if the microcredential is still valued, should be retired, or a new microcredential should be used.

Provide Context for Acquiring Third-Party Credentials

The Google Cybersecurity Professional Certificate provides students with foundational knowledge that can help them earn other industry credentials. For example, the CompTIA Security+ certification is widely recognized by employers and often required for employment. It is critical that faculty and staff are able to explain how the Google certificate can provide students with important knowledge and skills to earn the Security+ certification, or similar credentials. Earning the Security+ certification before graduation is critical to be competitive in the labor market today.

Support Faculty Engagement

As part of its faculty engagement strategy, the Division of Academic Innovation is launching a peer learning network and establishing a microcredential institute. These initiatives are designed to cultivate a community of practice where faculty can explore, experience, and exchange best practices around aligning or creating microcredentials. This sort of collaboration empowers faculty to share what works, navigate implementation challenges together, and experience microcredentials firsthand—so they are better equipped to design meaningful learning experiences that best resonate with students.

Conclusion

Microcredentials are used to meet a variety of needs that range from rounding out and enriching a degree program, fostering persistence and retention, demonstrating competency in technical skills, to enhancing employability outcomes. This case study provides an example of a course that integrates two courses from a third-party credential, in this case the Google Cybersecurity Professional Certificate, and maps the other courses in the Google certificate to other courses in the curricular pathway. By combining various types of credentials, students gain the deeper concepts from an academic degree and specific skills from a microcredential, which benefits students, faculty, and employers.

"These credentials can enhance resumes and provide practical skills for immediate workforce application. By integrating industry-recognized certificates, we ensure our students are career-ready and impactful from day one. I am proud of the opportunities we provide and the bright future we are building together."

– Mario Vela, assistant vice provost of career-engaged learning and executive director of the University Career Center, UTSA