



Clinic Development Toolkit



CLTC

Center for Long-Term
Cybersecurity

UC Berkeley

Sarah Powazek
Program Director of
Public Interest Cybersecurity

June 14, 2023

Table of Contents

Introduction

Why you should start a cybersecurity clinic



A good foundation

Three things you need to start a clinic



Designing your Clinic



Identifying, Creating, and Sustaining Clinic Funding



Liability

Reducing Risk for Institutions and Clients



What to teach

A menu of Curricula



Clinic Kickoff

Test-Runs and Improvement



Introduction



Why you should start a cybersecurity clinic

A Choose-Your-Own-Adventure Toolkit for Cyber Clinics

This guide is a result of months of collaboration, and years of learning and experimentation, from academic institutions within the Consortium of Cybersecurity Clinics to provide concrete advice on how to start up a cybersecurity clinic. There are many different ways to implement a clinic successfully, as it is adaptable to institutions of different sizes, resources, and degree programs — thus this toolkit will present a menu of options for new institutions to choose from, and examples of how each has succeeded.

The Consortium sincerely hopes that new institutions will find this toolkit helpful, and will consider starting one of these excellent programs in their communities. Academia is a powerful force for change, both to lift up students and to assist community organizations, and the journey to a cyber clinic begins here.

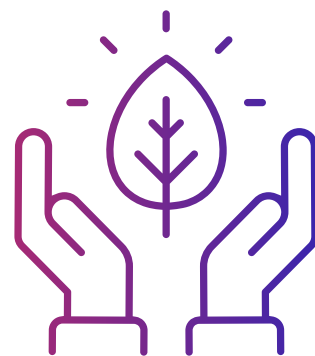
For decades, students at schools of law and medicine have gained hands-on training while helping outside clients and patients. But in the last five years, the “clinic” model has been adapted for the field of cybersecurity, and interest in the movement is exploding.

University-based cybersecurity clinics have become hubs for cyber learning in higher education and are poised to become a primary pillar of cyber talent. Clinics attract students from diverse academic backgrounds and train them in cyber civil defense by consulting with real clients. Clinics also promote a shared responsibility model for protecting under-resourced organizations by encouraging students to serve their local communities and instilling a sense of public service.

Providing Critical Hands-On Services to Community Organizations for Free

There is no substitute for face-to-face discussions to build lasting cyber resilience at under-resourced organizations, but many of these organizations cannot afford costly consulting services. Clinics fill this gap by providing proactive assessments to public interest organizations currently underserved by the cyber market. Faculty and instructors train students to provide services like risk assessments, incident response plans, penetration testing, ransomware training, and tabletop exercises.

As with law school and medical school clinics, these cybersecurity clinics serve under-resourced organizations that could not otherwise afford these services at market rates.



Introduction

Why you should start a cybersecurity clinic

Training A Multidisciplinary Group of Students for Cybersecurity Careers

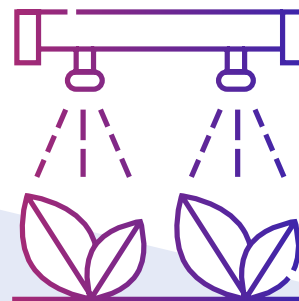
Clinics are constantly expanding the pool of cybersecurity talent within universities beyond cyber degree programs. Clinic programs shift the focus of cybersecurity from protecting assets to protecting people and communities; this broad mission connects to students' sense of purpose and attracts both STEM and non-STEM participants with more diverse backgrounds than traditional cyber programs.

Clinics serve communities where students live and consult with institutions that they care about. At MIT, where the clinic is situated within the Urban Planning department, students who care about improving city infrastructure join the clinic, which provides a gateway into the cyber field. UC Berkeley focuses on politically targeted nonprofits and thus interests students from Berkeley's Human Rights Center in addition to cyber master's students. The IU Bloomington Clinic is housed at the Nobel Prize-winning Ostrom Workshop, which has been an interdisciplinary hub of governance research for nearly 50 years and draws students from across three different degree programs.

Promoting Volunteerism and Providing Pipelines to Public Service

Clinics promote a model of shared responsibility for protecting under-resourced organizations and giving back to local communities. Participating in clinics embeds the value of public service into future cybersecurity leaders, and program alumni often reach out to clinics to ask how they can continue volunteering in their professional careers.

Working at a clinic also provides students with a direct opportunity for employment at public interest organizations. Now more than ever, municipalities, nonprofits, and hospitals need cyber talent, and clinics provide a talent pool with passion for, and experience in, working in these sectors. While many clinic alumni choose to join the private sector, several were employed by their former clients to continue their work.





A Good Foundation

What You Need to Start a Clinic

After seeing many clinics start up, and many others stop before becoming a reality, the Consortium has found several key institutional ingredients for a successful clinic. If your institution has many of these ingredients, chances are you are well suited to create and sustain a cybersecurity clinic.

1. Committed Faculty Champion



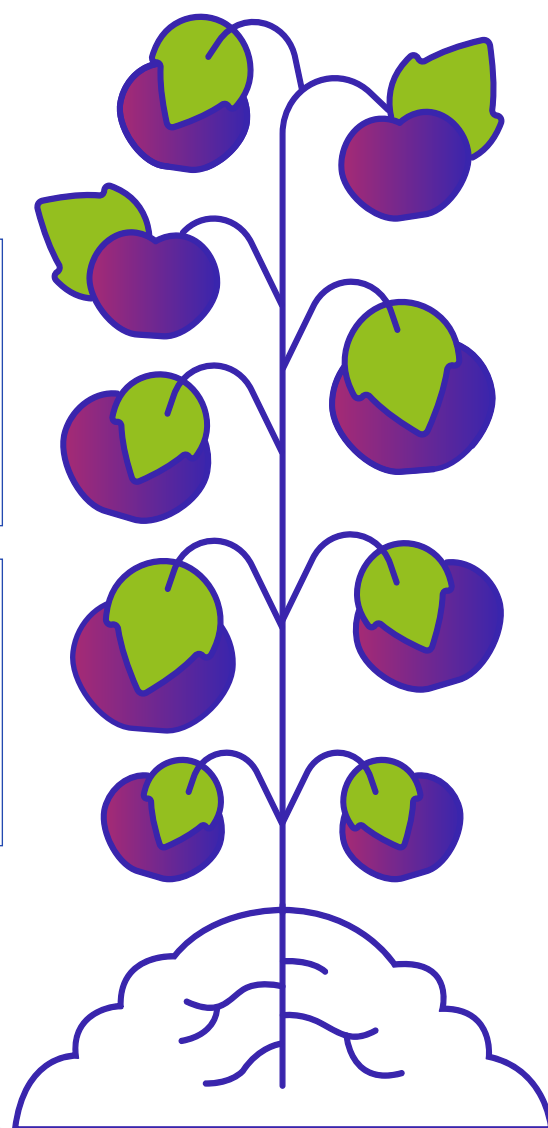
2. Interdisciplinary Institutional Support



3. Clinic Vision



4. Local Partners



1. Committed Faculty Champion(s)

Many clinics in the Consortium began by having a single faculty member champion to ideate, generate institutional buy-in, and seek out funding for the clinic. In particular, having a champion that has support from administrative and academic leadership and flexibility to orient their teaching, research, and service toward a clinic extra time is critical for coordinating the many components of starting up a clinic.

Creating a clinic can take up many hours of service work over several months to years, and thus may be best suited for senior faculty or other teaching roles who do not have to worry about tenure-track merit reviews and the competitive research pressures of junior faculty. Senior members may also be more familiar with the university administration and resources.



Examples of Faculty Champions

University of Georgia:

Mark Lupo championed the cybersecurity clinic model at UGA. After a search to revamp the existing CyberArch program at UGA, Mr. Lupo found the MIT Cybersecurity Clinic webinar and MIT Extension course, Cybersecurity for Critical Urban Infrastructure. He realized that the cybersecurity clinic model could improve upon the existing CyberArch program; it could condense the timeline for working with community organizations, and it relied on students to conduct the assessments. Mr. Lupo worked internally at UGA to gain support for the program and ultimately received funding to turn the CyberArch program into a cybersecurity clinic.

2. Institutional and Interdisciplinary Support

Cybersecurity Clinics sometimes require large institutional efforts, such as creating a new course in the catalog, or securing funding and teaching resources from the school. Thus many successful clinics gained early institutional support from key academic administrators for their clinics to launch the programs.

Consortium members also strongly encourage gaining interdisciplinary allies early in the process, as cross-listing clinic courses and/or inviting participation from many degree programs help expand the student talent pool for clinics. Not all schools have cybersecurity degree programs, but all students have cyber aptitude; it takes a variety of skills to learn the basics of cybersecurity.

Nearly every existing clinic program is open to students from different programs across campuses and encourages students of all backgrounds to participate. For instance, both Indiana University and UC Berkeley have open programs to all students—graduate and undergraduate—from all degree programs, which include students from business, law, and social science majors.



Example of Interdisciplinary Institutional Support

Prof. Larry Susskind believes that interdisciplinary support at his MIT Cybersecurity Clinic is key to their success. The program is run out of the Department of Urban Studies and Planning, drawing many students from that degree, and is cross-listed in the Computer Science Department. This encourages students from Computer Science to participate, as they can receive credit towards their major requirements, which are often strict and do not allow for many elective courses. Prof. Susskind says that gaining allies within the Computer Science Department was critical in getting the clinic course cross-listed and allowing more students to participate.

3. Clinic Vision

There are many different models for creating a cybersecurity clinic, and it is important to decide on a clear clinic vision before starting up the program.

This vision will answer questions such as:

- What community clients should the clinic serve, and how does this align with the goals of the host institution and host department?
- What benefit will the program provide to students at the institution, and how can it become an impactful experience for students?
- What sorts of resources, both for teaching and funding, will the program require, and why?

Consortium members recommend taking a look at existing models and identifying which components best suit an individual host institution. These decisions can be pulled together into a vision document that is then socialized throughout the institution to gain critical internal buy-in.

Finalizing a clinic vision can be very time-consuming. Some institutions reported frequent back-and-forth on issues like legal protection, space for meetings, events, and training, which services to offer, how to train students, what prerequisites students need, how to get clients, and how to recruit new students. In each case, this took several months to sort out. Most importantly, the stakeholders for these questions include program directors, student suggestions, administrators, other faculty, and even outside clientele.

Luckily, no one has to start from scratch; several popular clinic models are detailed in the next section, “Designing Your Clinic”.



4. Local Partners

Local partners can be a boon to a new clinic by connecting it to organizations in need. Many clinics partner with local hubs that serve as trusted partners, vouching for the quality of the clinic program to potential clients, and finding clients that would most benefit from the free services. The inclusion of a local partner in a funding proposal may also make the proposal more likely to be accepted, as it vouches for the longevity of the new clinic.

The best local partner to work with depends on the target clientele. For small businesses, the University of Nevada Las Vegas clinic works with the Nevada Small Business Development Center (SBDC).











For municipalities, the MIT Clinic works with the Massachusetts Cyber Center, an agency within the state government that works with municipalities, and Indiana University similarly partners with Purdue and the State of Indiana.





Designing your Clinic

There are many different programmatic models for creating a cybersecurity clinic at an academic institution. The success of each model depends on how well it suits the host institution's vision and existing infrastructure. The Consortium outlines a few common paths in this section and encourages new clinics to think deeply about the best way to implement each component of their program.

Clinic model		Class: clinics are taught as standalone classes, typically over a semester
		Capstone: a client consulting project is introduced in an existing class, with shorter engagements
		Club or Internship: clinics operate year-round and conduct long-term engagements and follow-ups
Clients to serve		Public entities: municipalities, hospitals, schools, libraries
		Nonprofits: food banks, refugee organizations, health clinics
		Small businesses: dentists, mom 'n pop shops
		Blend: two or more types of clients
Program instruction		Faculty-taught
		Faculty-advised, instructor-taught
		Mentor-supported

Choosing a Clinic Model

Successful operating models are run as one of the four following models: semester-long classes, capstone projects, student-led clubs, and internships.

Most cybersecurity clinics are run as **semester-long classes** during the academic year. Clinic champions create a new course in the academic catalog and often cross-list the class between departments to gain more interdisciplinary student participation. Students who take these classes are given course credit, either elective or towards their major requirements, in exchange for their services to the client.

Another clinic model is a **capstone project**, wherein a clinic component is tied into an existing class on cybersecurity or other topics. In this program, students may spend limited time working directly with a client, or do so for a specific project that may not encompass a full risk assessment.

Clinics can also be extracurricular activities. One clinic runs as a **student-led club**, where student leaders work with faculty advisors to identify clients and engage in long-term capacity-building efforts with them. Clinics can also be run as **internships**, where students participate outside class time for 1-6 hours per week and are compensated for their time.

Choosing Clientele to Serve

All clinics serve organizations that are “target rich, cyber poor” — typically small organizations that have few resources to defend against common cyberattacks. These organizations generally fall into these categories:

- **Local government:** Municipalities, school districts, libraries
- **Nonprofits:** Refugee organizations, faith-based nonprofits, food banks
- **Healthcare:** Medical clinics and small hospitals
- **Small businesses:** Restaurants, dentistry, and other local businesses

Some clinics choose to focus on a specific category of clientele. This allows instructors to customize teaching material, and for students to give more targeted advice based on common threats to clientele organizations. Other clinics keep a wide umbrella, serving several different types of organizations with risk assessments. As many of these organizations struggle with similar cybersecurity challenges, Consortium members have seen both of these models of choosing clientele succeed.

How did active clinics choose their model?

“The capstone project allowed for SIPA students to have a university-supported experience working on real-world issues”
— Columbia SIPA

“Path of least resistance to lock in a group of talented students was the main reason to do a class-based model as opposed to other variations.”
— University of Alabama

“We decided on the internship model due to the location of the program.... Though there is some limited ability to offer academic credit ... the more accepted model is to offer internships. As the UGA CyberArch program becomes more developed, the potential to offer credit courses for academic credit increases and might be pursued.”
— UGA

“We chose the class model to give us the most institutional support and longevity”
— Indiana University

How did active clinics choose their clientele?

UC Berkeley has a longstanding commitment to free speech and social justice and has a renowned Human Rights Center that researches war crimes and other serious violations of international humanitarian law and human rights. So UC Berkeley Citizen Clinic, in keeping with Berkeley's mission, serves nonprofits at risk of politically motivated cyberattacks, such as refugee organizations and nonprofits prosecuting war crimes.

— UCB

“Being located within CVIOG [Carl Vincent Institute of Government], which serves city/county/state governments, the natural focus of our current clients is in city/county governments, K-12 school systems, and rural hospitals.”

— UGA

“SIPA works with any clients from public agencies (from the local to national level), international NGOs and multinational organizations, and major firms in the private sector to answer a specific question framed by the client (which SIPA advises them on)”

— Columbia SIPA

Choosing Clinic Facilitation

Finally, all clinics are advised or led by staff or faculty. Some clinics are led and taught **directly by faculty**, who become a one-stop-shop for decisions on the clinic curricula, working with partners, and potentially getting the clinic listed in the course catalog. This facilitation model works particularly well if a faculty member is the clinic champion, and if the host institution is willing to allot part of the faculty member's time towards teaching the clinic. Clinics taught by faculty are often supported by one or more student TAs, PhD students, or postdocs.

Other clinics are taught primarily by, or supported by, **an instructor or lecturer**. While the term varies depending on the institution, instructors are often hired for specific teaching engagements and often are not able to engage in other clinic programs such as working with the Consortium of Cybersecurity Clinics. Instructors from industry help teach specific technical information such as how to conduct a risk assessment, particularly if an institution doesn't have a faculty member with cybersecurity expertise.

A few clinics have seen success in incorporating **volunteers** from the private sector to boost student support during client engagements. The University of Texas at San Antonio Project Xander partners with the MITRE Corporation, and MITRE volunteers mentor student teams and answer technical questions as students work through client assessments.

Identifying, Creating, and Sustaining Clinic Funding



Funding sustainable resources for a clinic can be a determining factor for a clinic's success. Thankfully, the unique strengths of the clinic model make for a compelling fundraising case for support, and existing clinics have helpful advice on best practices and resources to inform your fundraising plan.

Estimate Your Budget Needs

The cost of clinic startup and operations depends on faculty teachers, paid student internships, materials, enrollment, and full-time support staff or TAs. Consortium clinics have found that \$300k is a good funding target for the first year, and \$100k each year thereafter. After the first four to five years, some clinics can blend their budget with the host institution or department budget after proving value to students and community members.

Some clinics can operate with yearly budgets as low as \$75,000 and as high as \$300,000. The majority of clinic costs are paying instructors, including faculty time, lecturers, and TAs. Additional costs include administrative assistance, travel, and events, tools for the clinic, paying student interns, and other teaching materials.



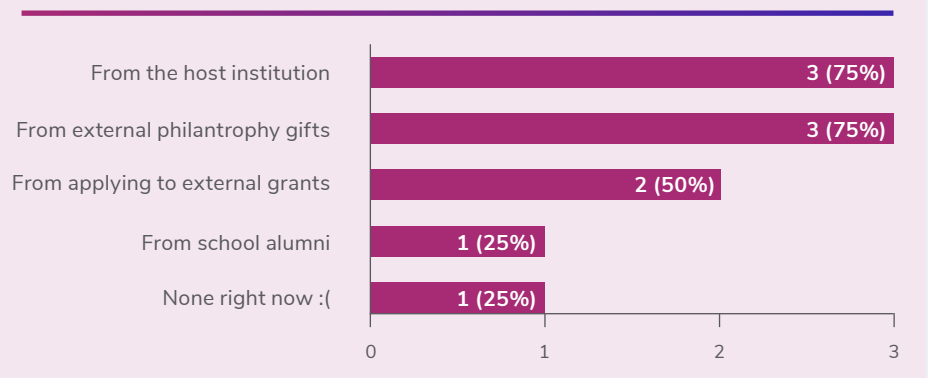
Here are some typical line items for a clinic budget:

- Faculty and instructor paid time for the clinic, can include summer salary
- Graduate researcher / TA / Post-doc for clinic teaching assistance (often 1 TA per semester)
- Equipment: Laptops and security keys, software for analysis, secure storage and collaboration
- Curriculum development expenses
- (Optional) Student travel to meet with clinic clients in person
- (Optional) Budget for student travel to conferences
- (Optional) Time with institution's communications staff to raise awareness, recruit students, celebrate clinic successes
- (Optional) Paying students as interns

Below are where some existing clinics draw funding from (some draw funding from several of these categories):

Where does your program receive funding from?

Choose all that apply (4 responses)



Host Institution Funding

Clinics with particularly strong administrative support from their host institution or department can operate, in part or in full, from institutional funds. In some cases, clinics can draw funding directly from their host department or receive a portion of funding from student tuition. In others, clinics can benefit from university-led fundraising on behalf of the clinic.

One opportunity, if a host institution cannot or will not fund the clinic, is to request matching funds from the host institution. Then, any resulting philanthropic funding received by the clinic would be doubled by the institution, ensuring the clinic is funded and has sustainable outside funding in addition to institutional support.

External Philanthropy and Grants

External philanthropic funding is an excellent opportunity to resource cybersecurity clinics. The Consortium recommends identifying and connecting with the fundraising personnel working with your school's academic unit to engage in discussion on the clinic model, share the proof of concept of existing clinic funders, and inquire about those individual, corporate, or foundation entities known to the fundraiser with an expressed interest in cybersecurity education, cybersecurity workforce development, public interest cybersecurity, and/or experiential learning programs.

Creating a one or two-page summary around the vision for the clinic that includes key personnel (who we are), planned activities (what we do), and a brief menu of giving tiers that correlate to clear impact (how you can help) can be a useful tool to open conversational doors within your home institution, with professional fundraising staff who can relay your message to prospective donors, and to begin discussions with potential funders.



Federal and State Funding opportunities

Several grant funding opportunities around the cyber workforce have appeared in recent years. Both the National Science Foundation (NSF) and the National Centers of Academic Excellence in Cybersecurity (NCAE-C) have funded programmatic grants reaching millions of dollars. Your host institution's office of government relations may also be able to point you to additional state funding opportunities.

Other Creative Funding Sources

Depending on the model of a cyber clinic, other funding pathways may be available. Some host institutions provide funding for student clubs, so club-based clinics like UNLV's Free Cyber Clinic can benefit from that funding. In some communities, industry partners may also support student clubs.

Persistence Pays

Fundraising often requires a significant investment of time and always requires persistence. Challenging trade-offs may emerge when fundraising pulls significant hours away from program coordination and teaching. The University of Georgia estimates that about 10% of the hours of one full-time faculty is devoted to fundraising. Other clinics report working to secure and steward funders, including providing reports and maintaining good donor relationships, is an ongoing component of their work.

Know that your efforts are part of a growing movement to develop — across the billions of philanthropic dollars devoted each year to peace and security causes — a new philanthropic arena: “cyberphilanthropy.” The Consortium of Cybersecurity Clinics welcomes your engagement to ensure that the trailblazing win/win design of cybersecurity clinics contributes to this inspiring vision.



Liability



Reducing Risk for Institutions and Clients

While this is a learning experience for students, their actions and recommendations have real effects on clients, with potential resounding implications for local communities. It is of the utmost importance that the clinic and its clients understand these impacts and take steps to both shield students and host institutions from liability and handle client engagements with integrity.

Current cybersecurity clinics have found it useful to involve the host institution's legal team early in the process of setting up a clinic. In-house counsel plays a key role in approving clinic engagement models by drafting agreement language and scoping the role of the clinic to suit the institution's comfort.

Protect Host Institutions and Students

Setting Expectations with MOUs

Institutions of higher education tend to be risk-averse, and concerns around cybersecurity clinics often rest on whether the institution will be held liable for any future cyber incidents suffered by clients that students assist.

Many cyber clinics find the use of Memorandums of Understanding (MOUs) (also called Statements of Expectations) to be particularly helpful in clarifying expectations for both the institution and the client. These MOUs are typically developed by host institutions and approved by campus legal departments and other key stakeholders and are presented to potential clients to sign before engaging with the clinic.

The Consortium of Cybersecurity Clinics has examples of MOUs used at different institutions that are provided to Consortium Members interested in starting up clinics.

Consider Protecting Student Identities

It is important for students to understand the risk of working to defend against cybercriminals. If a clinic is considering working with international clients, with clients facing political risks, or are working more hands-on within client infrastructure, that clinic should consider protecting student identities. For example, at UC Berkeley, students use pseudonyms when working with clients.



Serve Clients with Integrity

Community organizations are in a vulnerable position as targets for cyberattacks that lack sufficient resources to protect themselves. It is crucial that cybersecurity clinics, both leaders and students, take client work extremely seriously and work to build a trusting relationship with client organizations.

Select and Train Students for Sensitive Work

Clients should be assured that they will work with students who will handle sensitive information with care and who have enough knowledge to provide them with assistance. To build client trust and vouch for student integrity, host institutions sometimes conduct background checks on prospective students before accepting them. These background checks can be done in collaboration with the campus police department.

Once a student has passed the background check, then they may begin the training work required to ensure that a student has the tools necessary to work with clientele. Note that some clinics do not require background checks for students.

Every active clinic trains students in some capacity to be able to perform helpful cyber assessments and services for clients. More information on training curricula can be found in the next section.

Communicate and Collaborate Securely

An integral part of client work is ensuring the security and confidentiality of sensitive client information. Many clinics choose to employ a secure cloud hosting platform to share documents on. This tool makes it easy to give students and clients access and remove access and documents after an engagement has ended.

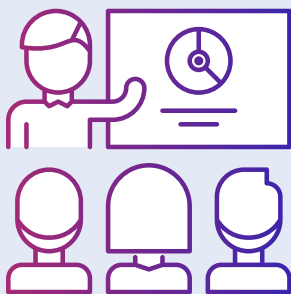
For communication, some clinics use encrypted messaging platforms and/or conduct client communication primarily in person or over video conferencing.

Data scrubbing is also an important part of client work; clinics may choose to remove client names and identifying information from final reports to keep student work available as examples without identifying past clients. Clinic leadership should also counsel clients not to share any sensitive information such as PII, health information, employee records, credit card information, or financial records.

It is important to never publicly release information about a client's cyber vulnerabilities, highly restrict access to this information during an engagement, and remove access and scrub client identifying information after an engagement. Poor handling of this sensitive information could result in targeted cyber threats toward a client organization.

Liability Advice from Clinics

Talk to your institution's legal department immediately after initial talks with your department. Legal can be a LONG challenge, so do not underestimate the time required.
— University of Alabama





What to teach

A menu of Curricula

The heart of cybersecurity clinic operations is the curriculum. Each host institution goes about this process very differently, and each takes pride in customizing cybersecurity content for its student body and clientele.

But now that clinics have been in operation for several years, there is no need to reinvent the wheel! This section contains resources about what clinics usually teach, and where they pulled curricula topics from.

Typical flow of curricula



Prerequisites for Students

Since curricula vary widely between educational institutions, there is no one-size-fits-all set of prerequisites for students to participate in a cybersecurity clinic. Some institutions have no prerequisites at all, and students from all degree programs and majors are welcome to join. Other programs require prerequisite courses in English, Mathematics, and Statistics that qualify mainly undergraduate Juniors and Seniors. Others still have requirements such as being enrolled in a specific degree program, having a GPA over a particular cutoff, taking a cybersecurity training course, or passing a certification exam.



Training Students

to teach students of different skill levels and interests, and to ensure that clients find student work valuable, all clinics devote time to training students before allowing them to work with clients.

While the exact training varies, the goals are the same; to teach students basics of cybersecurity risk, and to prepare them to run an assessment with a real client. Both MIT and UGA utilize the [MIT Critical Urban Infrastructure](#) course to train students for their cybersecurity clinics and students at MIT must pass the course exam before they can work with clients. This online video lecture course is available online for free and is accessible to any new clinics interested in a plug-and-play training course who will be serving organizations like cities and hospitals.

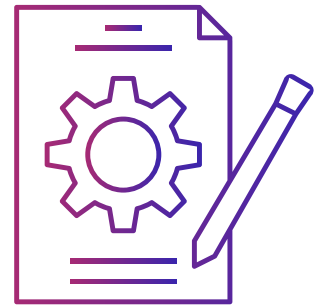
UC Berkeley uses the first six weeks of the clinic class for student training on topics like policy, cybersecurity frameworks, business administration/project management techniques, and some legal studies. Students also review collaboration tools, learn how to do open-source intelligence research and learn a module on “psychological resilience” and how to handle topics outside of a student’s life experiences.



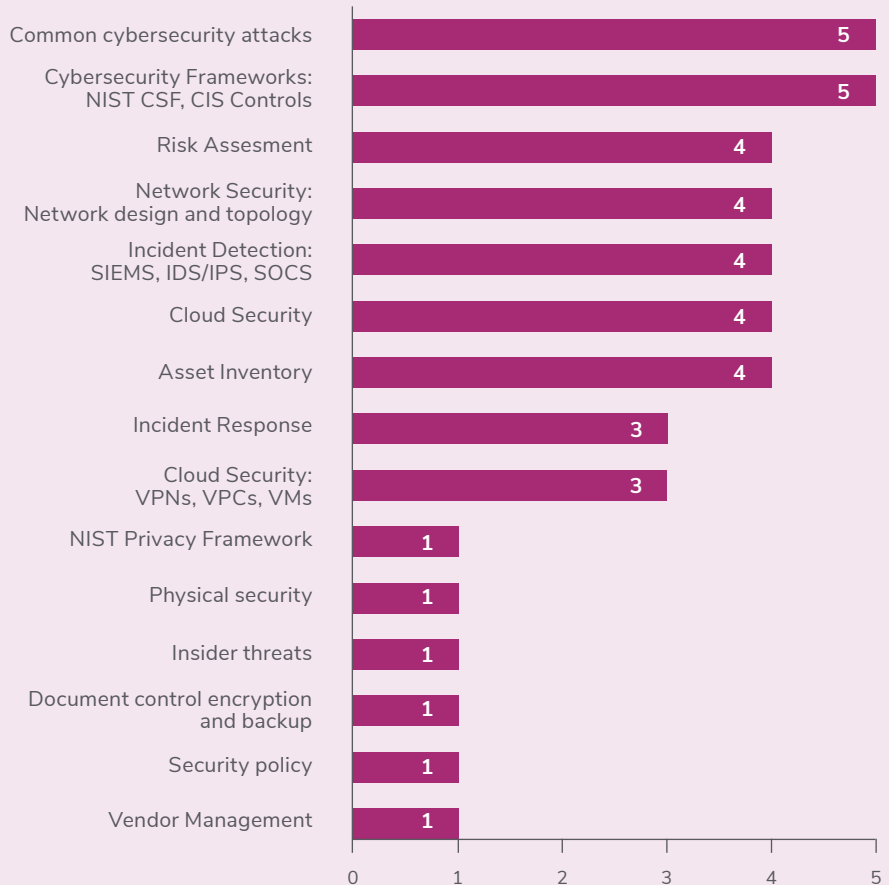
Core Curricula Topics

The first few clinic programs developed almost completely-custom curricula. Over the years, new clinics and established clinics alike have borrowed topics from popular cybersecurity frameworks and other resources to teach students the latest cybersecurity best practices.

Below is a chart of the most common topics taught across different clinic curricula. Full syllabi are not included here but are available upon request for members of the Consortium. UC Berkeley’s Citizen Clinic curriculum is [available online](#).



Common Cybersecurity Clinic Curricula Topics



Clinic Engagement Frameworks

In addition to teaching students basic cybersecurity topics, clinics each employ a slightly different framework for analyzing cybersecurity risk of clients. Some clinics run a completely custom risk assessment and adjust the questions students ask clients each year as the clinic learns more. Other clinics base their assessments on common frameworks such as the NIST Cybersecurity Framework (CSF) or the CIS Critical Security Controls (CIS Controls), and while some run hands-on engagements with clients, such as performing vulnerability scans on client networks.

For example, MIT has developed a custom assessment of over ___ questions, pared down from hundreds of questions in the NIST CSF. UTSA also utilizes a custom assessment framework called the [Community Cyber Security Maturity Model \(CCSMM\)](#). Currently, none of the custom assessment frameworks used by cybersecurity clinics are available for free online, though MIT's custom security assessment can be shared upon request for members of the Consortium.

More information on common curricula resources can be found on the Resources list.



Resource	Learn More At
CIS Critical Security Controls (CIS Controls)	https://www.cisecurity.org/controls
CISA Cyber Resilience Review (CRR)	https://www.cisa.gov/resources-tools/resources/cyber-resilience-review-downloadable-resources
CISA Cyber Security Evaluation Tool (CSET)	https://www.cisa.gov/downloading-and-installing-cset
CompTIA Security+ Certification	https://www.comptia.org/certifications/security
Microsoft Certification: Security, Compliance, and Identity Fundamentals	https://learn.microsoft.com/en-us/certifications/security-compliance-and-identity-fundamentals/
MIT Cybersecurity for Critical Urban Infrastructure	https://learning.edx.org/course/course-v1:MITx+11.S198x+3T2022/home
NIST Cyber Security Framework (CSF)	https://www.nist.gov/cyberframework
NIST NICE Framework	https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center
NSA Centers of Academic Excellence in Cybersecurity (CAE-C) Knowledge Units	https://public.cyber.mil/ncae-c/documents-library/
The Texas A&M Engineering Extension Service (TEEX)	https://teex.org
UTSA Community Cyber Security Maturity Model (CCSMM)	https://cias.utsa.edu/research/maturity-model/



Clinic Kickoff

Test-Runs and Improvement

Once clinics receive administrative support, it takes around 9 months to work on internal training, policies, and curricula before the clinic can officially launch. After clearing numerous administrative, legal, and financial hurdles, it is finally time to start the clinic.

Running a Clinic Pilot

Once the program policies are in place, clinic instructors should consider beginning with a pilot run; instructors ran a smaller-than-normal class to test the curriculum and engagement, and students gave regular feedback on how the course needed to improve.

In some cases, clinics were able to run a pilot program within an existing institute program or course, allowing the program to go through a smaller scale of testing without officially launching a new program or cohort. This can also help build internal buy-in as clinic facilitators collect positive student feedback and gauge interest in a standalone program.

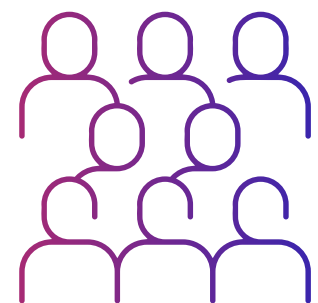
Here are few examples of how clinics run pilot programs:

- 1** **University of Georgia:** Dr. Paul Brooks, Associate Vice President for PSO, led the CyberArch committee in a pilot program that began in early 2018 with two counties within the Archway Community program. Each Archway community has an embedded UGA faculty member and an Archway professional to assist community leadership in connecting with UGA resources to assist with strategic community initiatives.
- 2** **MIT:** The MIT clinic did a pilot run with a single client. Each week the client and the students assisted in testing and refining all of the clinic coursework and materials. At the end of the pilot, the entire curriculum was revamped from pilot feedback.
- 3** **UC Berkeley:** The UC Berkeley Citizen Clinic first offered the clinic course as a pilot in-person for all departments in the spring of 2018. After the success of the pilot, the Citizen Clinic has been running every Fall and Spring semester.

Joining the Consortium

We hope this Toolkit has been useful, and that many more academic institutions will pursue clinical education in cybersecurity. The most up-to-date information about public resources and funding announcements will be available on the Consortium website (<https://cybersecurityclinics.org>).

As of 2023, the Consortium of Cybersecurity Clinics hosts quarterly Introduction Calls for all educational institutions worldwide interested in starting up a cyber clinic. We encourage folks interested in learning more to join us and share in our goal of a cyber clinic in every U.S. state by 2030.





**The Consortium of
Cybersecurity Clinics**