



Katz

Katz School
of Science and Health

Katz School Master of Science in Cybersecurity (30 Credits)

Program Director – Prof. Sivan Tehila

Program Overview

The Master of Science in Cybersecurity is a comprehensive, single-track graduate program designed to prepare professionals for technical, governance, and leadership roles across the cybersecurity workforce. The program integrates foundational and advanced cybersecurity knowledge with applied practice, emphasizing alignment with nationally recognized standards and frameworks.

The curriculum is explicitly aligned with:

- **NIST Cybersecurity Framework (CSF 2.0)**
- **NIST Risk Management Framework (RMF) and SP 800-series**
- **NSA / DHS Centers of Academic Excellence in Cyber Defense (CAE-CD) knowledge units**
- **NICE Workforce Framework (NIST SP 800-181)**

The program also incorporates **AI-enabled cybersecurity concepts**, hands-on learning, and experiential opportunities to ensure graduates are workforce-ready and capable of adapting to evolving threat landscapes.

Program Learning Outcomes

1. Explain current standards and practices in cybersecurity and how they are applied to cyber exposures and threats, including systems design, methods, and techniques aimed at prevention, mitigation, response, and recovery from cyber-attacks and intrusion.
2. Develop a risk-based approach to managing operational factors associated with cybersecurity.
3. Explain operating system security architecture concepts, including integrity and access control based security models and design, kernel protection, trusted platform module, and security auditing.
4. Discuss the importance of operating system, embedded system and application testing for errors, and vulnerability and defect testing methodologies
5. Assess the importance of real-time internal hardware and software intelligence and the steps an organization must take to develop a comprehensive risk management strategy and policy.
6. Apply communication techniques to inform management of the need for IT Risk Assessment and Management procedures. Apply communication techniques to inform management of the need for IT Risk Assessment and Management procedures.

Katz School of Science and Health, Yeshiva University

P: 646.592.4753 katz@yu.edu yu.edu/katz

Israel Henry Beren Campus, 205 Lexington Avenue, 6th Floor, New York, NY 10016



Katz

Katz School
of Science and Health

Program Structure (30 Credits)

- **Core Requirements:** 8 courses / 24 credits
- **Electives:** 2 courses / 6 credits

Core Requirements (24 Credits)

CYB 5000 – Cybersecurity Foundations (3 Credits)

This course will prepare students for in-depth study and competency building in cybersecurity. Through hands-on work in understanding and applying cybersecurity frameworks and guidelines, students will explore general concepts, current standards and practices, and terminology. Students will be introduced to the most common cybersecurity functions, current and emerging cyber threats, challenges, and solutions. The course will engage students in basic solutions design and applying techniques, using current case studies to introduce them to the operational factors, both non-technical and technical that address exposures and responses to cyber threats.

Framework Alignment:

- NIST CSF: Govern, Protect
- NIST RMF: Prepare
- NSA CAE-CD: Cybersecurity Foundations, Policy & Ethics

CYB 5100 – Architecture of Secure Operating Systems, Applications, and Devices (3 Credits)

As innovations involving sensing technology, robotics, and the Internet of Things are more frequently deployed in organizations, on vehicles, or around the home, businesses and personal safety can be highly dependent on the secure architecture of technology. Students will learn key concepts about technology access control design, fault and tamper resistance, testing, and common criteria used to determine if technology solutions are robust enough to withstand attacks such as tampering, denial of service, and unauthorized access.

Framework Alignment:

- NIST CSF: Protect
- NIST RMF: Select, Implement
- NSA CAE-CD: Secure Computing, Platform Technologies



Katz

Katz School
of Science and Health

CYB 5200 – Network, Data, and Communications Security (3 Credits)

Having a solid defense-in-depth strategy for architecting and operating networked technology provides organizations with operational resilience from cyber-attacks and data breaches. Students will learn key concepts about security architecture, network segmentation, defense-indepth, encryption technologies, and backup/replication sites, including cloud-based servers and services.

Framework Alignment:

- NIST CSF: Protect, Detect
- NIST RMF: Implement
- NSA CAE-CD: Network Defense, Cryptography

CYB 5300 – Risk Management and Cybersecurity (3 Credits)

This course takes a multi-disciplinary approach to the study of risk governance and cybersecurity. Students will learn how to analyze, assess, control, and manage cybersecurity risks from the individual to the operational level. They will develop practical knowledge, analytical skills, and mathematical methods for calculating risk, as well as the artistic skills required to make decisions about which risks to control and how to control them.

Framework Alignment:

- NIST CSF: Govern
- NIST RMF: Prepare, Select, Assess
- NSA CAE-CD: Risk Management, Cyber Defense

CYB 5400 – Cybersecurity Audit, Assessment, and Training (Cloud Security) (3 Credits)

This course will teach students how to assess and evaluate cyber security risks, conduct computer security audits, and test preparedness and response levels in the current technology environment. The course will explore standard evaluation and testing methodologies currently used across industries to identify and address cyber security threats. Students will also study current cyber policies used in both private and public sectors and their implementation.

Framework Alignment:

- NIST CSF: Govern, Assess
- NIST RMF: Assess, Monitor
- NSA CAE-CD: Cyber Defense Operations

Katz School of Science and Health, Yeshiva University

P: 646.592.4753 katz@yu.edu yu.edu/katz

Israel Henry Beren Campus, 205 Lexington Avenue, 6th Floor, New York, NY 10016



Katz

Katz School
of Science and Health

TMG 5500 – Leading Technology Organizations (3 Credits)

Successful leaders require more than technical knowledge and skills: they must be able to identify and prioritize strategic challenges and opportunities and champion initiatives to address them. Students will master strategies for building short- and long-term plans, developing a culture of productivity and excellence, leading high performing teams, strengthening organizational communication, leading change management initiatives, and enabling the leadership potential of others. Additional topics may include individual and group behaviors, interpersonal relationships, and organizational structure and design. Importantly, students will learn the science behind strategic leadership in agile, high performing technology organizations.

Framework Alignment:

- NIST CSF: Govern
- NICE Workforce: Leadership & Oversight Roles

CYB 7992 – E-Discovery, Digital Evidence, and Computer Forensics (3 Credits)

Electronic discovery has become a critical component of all major litigations as the key evidence increasingly consists of e-mail and electronic documents. This course will teach students the law of E-discovery, practical best practices provide exposure to the technology behind it all. The focus will be on making students competent as to the legal obligations of e-discovery.

Framework Alignment:

- NIST CSF: Respond, Recover
- NIST RMF: Monitor
- NSA CAE-CD: Incident Response, Digital Forensics

CYB 6500 – Cybersecurity Capstone (3 Credits)

In this course, students integrate the skills developed in previous classes into a comprehensive body of knowledge and provide tangible evidence of these competencies. The Capstone has four components: 1) a brief proposal and project schedule; 2) the main project deliverable; 3) a final presentation; and 4) a reflection on the student's cybersecurity management skills and competencies, with some depth in one or two areas of the profession and grounded in a particular real-world context.

Framework Alignment:

- NIST CSF: Protect, Detect, Respond, Recover
- NIST RMF: Full Lifecycle

Katz School of Science and Health, Yeshiva University

P: 646.592.4753 katz@yu.edu yu.edu/katz

Israel Henry Beren Campus, 205 Lexington Avenue, 6th Floor, New York, NY 10016



Katz

Katz School
of Science and Health

- NSA CAE-CD: Capstone / Advanced Cyber Defense

Electives (6 Credits)

Students complete **two elective courses** (6 credits). One elective may be substituted with an approved internship.

CYB 6300 – Special Topics- Cybercrime, Cyberwar, and Threat Actors (3 Credits)

This course provides the opportunity to offer boutique short-term courses on emerging phenomena, policies, processes, technologies, and techniques in cybersecurity. The expectation is that this will be an advanced class that requires an appropriate student project and deliverable in line with the number of credits awarded for the course.

Framework Alignment:

- NIST CSF: Detect, Respond
- NSA CAE-CD: Cyber Threats, Cyber Operations

CYB 6400 – Cybersecurity Internship (3 Credits)

This course consists of an off-campus internship experience supervised by a staff person at the internship site and overseen by a faculty advisor. The internship site must be approved by the program director, and the overall duration of student work must be no less than 150 hours (based on a 3-credit course). At the start of the internship, the student and faculty advisor will jointly develop specific learning objectives tailored to the nature of the internship. Over the course of the internship, students will be required to submit weekly reflections, and at the end of the internship, students write a final paper that represents the culmination of the work performed.

Framework Alignment:

- NICE Workforce Framework: Applied Practice
- NIST CSF: Role-dependent