INTERDISCIPLINARY INFORMATICS (Si2)

The mission of the School of Interdisciplinary Informatics (Si2) is to provide students and faculty the opportunity to pursue their passions, to use technology in all its facets, and to be transformative. We collaborate to deliver individualized education, world class research, and immersive experiences to create and harmonize knowledge from multiple disciplines.

The School of Interdisciplinary Informatics is a key driver in taking the College of Information Science & Technology (IS&T) to the next level. The School is a hub for technology innovation for undergraduate and graduate students. It provides opportunities for collaboration with other disciplines through sharing curriculum and collaborative applied research.

The School is also an 'IT solution-finding' resource for our community partners in the areas of cybersecurity, healthcare, bioinformatics, public health informatics, business, and government.

The School provides a unique opportunity for undergraduate students to integrate education, research, and outreach into their college experience. For example, many students have been involved in a public health informatics project that focuses on providing an emergency response system for public health laboratories. Students are able to earn academic credit working on this project and also have opportunities to do research and publish papers.

Faculty also engage students with community partners through our service learning initiatives. Students have worked with the Douglas County Correctional Center, KIDS Can! Alegant Health, Douglas County Health Services, and Nebraska Family and Children Services, to name a few.

These initiatives are a win/win situation for everyone involved: the students, the community partners, and the schools. Ultimately, they have a positive economic impact that flows throughout the community and the state.

The School of Interdisciplinary Informatics reflects the role and mission of UNO’s College of Information Science & Technology, The Peter Kiewit Institute, and the University of Nebraska at Omaha in a number of ways. It is a direct response to the opportunities and challenges presented by information technology as it relates to economic growth for the state and region in applied IT areas such as medical informatics and cybersecurity. The School encourages the enhancement and fostering of new educational, research and creative activities by bringing together practitioners, researchers and students in interdisciplinary fields of importance to the state and the University. The School is unique in the country and leads to increased national visibility of the University of Nebraska in the area of interdisciplinary applications of information technology.

The School of Interdisciplinary Informatics addresses the following needs and demands of our academic, business, and community stakeholders:

1. Promotion of growth of interdisciplinary areas;
2. Facilitation of innovative partnerships with external constituents, including leveraging the expertise of the local community;
3. Diversity of personnel;
4. Reduction of barriers to collaboration;
5. Flexible and agile structure for quick response to opportunities;
6. Solidification of regional and national recognition as an important resource for the study and advancement of IT in the domain of healthcare, biosciences, and information security;
7. Visibility of the college and its interdisciplinary focus;
8. A magnet for collaborative external funding;
9. Development of the next generation workforce to address local, regional and national needs in exciting, new interdisciplinary domains.

Second Baccalaureate Degree for Bioinformatics

General Requirements
Students who have satisfied the requirements for a first baccalaureate degree other than Bioinformatics at the University of Nebraska at Omaha must complete a minimum of 30 additional semester hours at the University for a second baccalaureate degree.

Bioinformatics Requirements (89 hours)
To obtain Bioinformatics as a second bachelor’s degree, students must complete academic requirements for the degree which include 24 credit hours of IS&T core courses, 11 credit hours of Math courses, 16 credit hours of Biology courses, 14 credit hours of Chemistry courses, and 24 credit hours of Bioinformatics courses. Students must consult an academic advisor in the College of IS&T prior to starting this program. Some transfer coursework may apply; however, 30 of the last 36 hours for the degree must be University of Nebraska at Omaha courses.

Second Baccalaureate Degree for Cybersecurity

General Requirements
Students who have satisfied the requirements for a first baccalaureate degree other than Cybersecurity at the University of Nebraska at Omaha must complete a minimum of 30 additional semester hours at the University for a second baccalaureate degree.

Cybersecurity Requirements (83 hours)
To obtain Cybersecurity (CYBR) as a second Bachelor’s degree, students must complete academic requirements for the degree, which include 9 credit hours of IS&T core courses, 21 credit hours of required Computer Science core courses, 30 credit hours of required Cybersecurity core courses, and 8 hours of Mathematics courses. Students must also complete 15 credit hours of required Cybersecurity electives. Students must consult an academic advisor in the College of IS&T prior to starting this program. Some transfer coursework may apply; however, 30 of the last 36 hours for the degree must be University of Nebraska at Omaha courses.

Second Baccalaureate Degree for IT Innovation

General Requirements
Students who have satisfied the requirements for a first baccalaureate degree other than IT Innovation (ITIN) at the University of Nebraska at Omaha must complete a minimum of 30 additional semester hours at the University for a second baccalaureate degree.

IT Innovation Requirements (87 hours)
To obtain IT Innovation as a second Bachelor’s degree, students must complete academic requirements for the degree which include 6 credit hours of Mathematics courses, 48 credit hours of required IS&T core courses, and 33 credit hours of area of emphasis courses. (Approval of the area of emphasis courses by the ITIN Undergraduate Program Committee is required prior to course enrollment.) Students must consult an academic advisor in the College of IS&T prior to starting this program. Some transfer coursework may apply; however, 30 of the last 36 hours for the degree must be University of Nebraska at Omaha courses.

Opportunities for Graduate Study

Integrated Undergraduate/Graduate Tracks (IUG) in Bioinformatics/Biomedical Informatics, Cybersecurity, and IT Innovation

The College of IS&T’s School of Interdisciplinary Informatics offers IUG tracks for the Bioinformatics/Biomedical Informatics, Cybersecurity, and IT Innovation programs.
The primary purpose of the IUG program is to provide outstanding undergraduate students in the College of IS&T an opportunity to complete a BS and an MS degree in five years. It is designed for dedicated students who are motivated and willing to take on the challenges related to graduate studies early.

Students majoring in Bioinformatics (BIOI) can complete the undergraduate BS in BIOI and the MS in Biomedical Informatics (BMI) in five years.

Students majoring in Cybersecurity can complete the undergraduate BS degree in CYBR and the graduate MS degree in CYBR in five years. Students pursuing undergraduate degrees in MIS or CS with an Information Assurance concentration may also be eligible for this IUG track option.

The College of IS&T has partnered with the University of Nebraska Medical Center’s College of Public Health to enable ITIN majors to complete a BS in ITIN and an MS in Public Health with a concentration in Biostatistics in five years.

Contact
For more information, contact the College of IS&T Academic Advising Office at 402.554.3819.

Website (http://www.unomaha.edu/college-of-information-science-and-technology/school-of-interdisciplinary-informatics/)

General Guidelines

IUG in Cybersecurity Program of Study
The CYBR IUG track is a 141-hour undergraduate-graduate option that allows eligible students to work toward the MS in CYBR degree requirements while completing their undergraduate degree. Students interested in this option will work closely with an academic advisor in the College of IS&T and a faculty mentor to develop an integrated plan of study.

Time of Admission to the Program
Students will be eligible for admission to the integrated degree program when they have completed their junior year in the College of IS&T; they can apply for consideration in the last part of their junior year. Students admitted to the program will start taking graduate courses in their senior year and are allowed to use a maximum of 12 hours of CYBR/CSCI/CIST 8xx6 courses toward the undergraduate degree.

Joint Admission
Students must apply to and meet the admission requirements of the graduate degree in Cybersecurity.

Plan of Study
In consultation with an academic advisor and a faculty mentor, students will be required to prepare a plan of study. The plan of study will cover the entire time period of the program and will be periodically reviewed with an advisor. Students admitted to the integrated degree program will be required to complete any applicable graduate foundation courses or their equivalent undergraduate courses during their junior/senior years.

Tuition Charges
Students will be required to pay graduate tuition rates when taking graduate courses.

Admission Requirements and Procedures
1. Students with junior standing and at least 85 hours of completed coursework in their undergraduate degree program may apply for admission consideration into the integrated undergraduate/graduate (IUG) track. Students pursuing undergraduate degrees in CYBR are automatically eligible to apply. Students pursuing undergraduate degrees in MIS or Computer Science (CS) with an IA concentration may also be eligible for this track option and can apply to the CYBR GPC for permission to apply.

2. At the time of application, students must have a GPA of 3.0 or above overall as well as in their major coursework.

3. Interested students will be required to present a portfolio of the following credentials, and whenever possible, this presentation will be made to the IUG Selection Committee. The portfolio is to include the following:
   a. Three letters of recommendation, at least two from faculty
   b. Statement of Intent: a personal statement about why the student wishes to apply for the IUG track
   c. Undergraduate transcripts
   d. Other supporting documents (e.g. resume, projects and papers, software, work experience, etc.) should be included where possible
4. All applicants will need to meet any other admission requirements established for the MS in CYBR program.

Additional Information
- The application to the IUG track will be considered as a complete package, and therefore, obtaining a high undergraduate GPA and/or a high GMAT/GRE score is not a guarantee of admission.
- Students are highly encouraged to identify and work with a faculty mentor who knows their background and can champion their application to the IUG track.
- Students are allowed to use a maximum of 12 hours of CYBR/CSCI/CIST 8xx6 courses towards the undergraduate degree.

Integrated Undergraduate/Graduate Track (IUG) in IT Innovation
The IUG in IT Innovation from UNO and the Master of Public Health (MPH) with a concentration in Biostatistics from the University of Nebraska Medical Center (UNMC) can be completed in five years. This IUG track is a 144-hour undergraduate-graduate option that allows eligible students to work toward the MPH degree requirements while completing their undergraduate degree in IT Innovation. Students interested in this option will work closely with an academic advisor in the College of IS&T and a faculty mentor to develop an integrated plan of study.

General Guidelines

Time of Admission to the Program
Students will be eligible for admission to the integrated degree program during their sophomore year in the College of IS&T and can apply for consideration after completing at least 48 hours of coursework in their undergraduate degree. Students admitted to the program will start taking graduate courses in their junior year and are allowed to use up to 21 credit hours of graduate courses toward the ITIN undergraduate degree’s area of focus.

Joint Admission
Students must apply to and meet admission requirements of the MPH graduate program.

Plan of Study
In consultation with an academic advisor and a faculty mentor, students will be required to prepare a plan of study. The plan will cover the entire time period of the program and will be periodically reviewed with an advisor.

Tuition Charges
Students will be required to pay graduate tuition rates when taking graduate courses.

MPH Program Requirements for Admission
- Completion of the UNMC MPH degree application.
- Three letters of the recommendation from academic or professional references.
First, they each have interdisciplinary components in their curriculum.

Second, they rely on working collaboratively with other disciplines and the community.

Third, according to the Bureau of Labor Statistics, all of these career areas have tremendous growth potential over the next ten years.

**Writing in the Discipline**

All UNO students are required to take a writing-in-the-discipline course within their major. Students must take CIST 3000.

**Minors Offered**

- IT Innovation Minor (http://catalog.unomaha.edu/undergraduate/college-information-science-technology/school-interdisciplinary-informatics-si2/itin-minor/)
- Cybersecurity Minor (http://catalog.unomaha.edu/undergraduate/college-information-science-technology/school-interdisciplinary-informatics-si2/cybersecurity-minor/)
- Bioinformatics Minor (http://catalog.unomaha.edu/undergraduate/college-information-science-technology/school-interdisciplinary-informatics-si2/bioinformatic-minor/)

**IT Innovation (ITIN) Minor**

The objective of the IT innovation (ITIN) minor is to provide students across the university with a substantive qualification in information technology to augment their respective majors and allow them to be even more innovative as to the application of IT to their learning and career choices.

**Cybersecurity (CYBR) Minor**

Cybersecurity is the practice of managing information-related risks by ensuring confidentiality, integrity, and availability of information. The minor will provide students across the University with an opportunity to earn credits in CYBR, and it will enable them to understand the nuances of everyday cybersecurity issues. The CYBR minor will also provide students an opportunity to strengthen their portfolio, resulting in increased job opportunities.

**Bioinformatics Minor**

Bioinformatics is a rapidly expanding interdisciplinary field focused on collecting, processing, and analyzing vast amounts of biological and biomedical data and has become an indispensable component of biomedical research. The minor in Bioinformatics offers an opportunity for students majoring in other disciplines to acquire the foundations of the field and add in-demand skills to their portfolio.

**Bachelor of Science in Bioinformatics**

Graduates from UNO’s Bioinformatics (BIOI) program in the College of IS&T will be able to use their preparation to apply and investigate technology to solve bioinformatics problems in a comprehensive, competitive and effective way. Students with an undergraduate degree in bioinformatics can expect to have a foundational knowledge in computer science, biology, statistics, and database administration.

The job outlook for Bioinformatics majors is excellent. Versatile and greatly in demand, our graduates have gone on to become programmers, data analysts, and senior-level scientists. Employment is available with private and public industries, research institutions, government institutions, non-profits, and universities around the globe. The Bioinformatics degree can also serve as a springboard to graduate work, opening the door to academic careers and other careers that require informatics skills coupled with biological background.

**Careers Options:**

- Bioinformatics Scientist/Analyst
- Scientific Curator
- Computational Biologist
Career Options:
- Entry Level
  - Cybersecurity Specialist/Technician
  - Cyber Crime Analyst/Investigator
  - Incident Analyst/Responder
  - IT Auditor
  - Secure Applications Developer
- Mid-Level
  - Cybersecurity Analyst
  - Cybersecurity Consultant
  - Penetration and Vulnerability Tester
  - Secure Systems Integrator
  - Cybersecurity Lead Programmer
- Advanced Level
  - Cybersecurity Manager/Administrator
  - Cybersecurity Engineer
  - Cybersecurity Architect
  - Chief Information Security Officer

Bachelor of Science in Cybersecurity
Cybersecurity (or CYBR for short) is a rapidly expanding field focused on keeping critical infrastructure, systems, and users safe. From collecting attacks on individuals to large-scale attacks on facilities like power plants, government systems, and industrial control systems, threats abound in the 21st century global economy. Adapting to these changing threat environments is a continual activity that companies, and governments must engage with. These organizations rely on cybersecurity practitioners to identify threats, determine risk, and implement mitigating protections in their software, hardware, and online systems — such as those on mobile, web and Internet of Things (IoT) platforms. It is also important to build protections into new software and hardware during the design and development process, track and monitor developed systems for on-going risk, and assess them forensically when something goes wrong. The CYBR degree program at UNO focuses on technical curricula that prepare students for pathways into a range of careers that address these topics.

Bioinformatics

BIOI 1000 INTRODUCTION TO BIOINFORMATICS (3 credits)
Bioinformatics is a scientific discipline that integrates mathematical and computational techniques with biological knowledge to develop and use computational tools to extract, organize and interpret information from genetic sequence data. The field is growing rapidly with the advancement in molecular technology to sequence the genomes of many different organisms. This course will provide an introduction to the field and will examine some of the problems of interest to bioinformaticians and how these relate to biology, computer science, mathematics and engineering. Topics will include an overview of the biology, mathematics and computer science needed to understand these tools.

Distribution: Natural/Physical Science General Education course

BIOI 2000 FOUNDATIONS OF BIOINFORMATICS (3 credits)
Bioinformatics is a new scientific discipline that integrates mathematical and computational techniques with biological knowledge to develop and use computational tools to extract, organize and interpret information from genetic sequence data. The field is growing quickly due to rapid advances in sequencing and other biological technologies that allow the genomes of different organisms to be easily sequenced. This course provides an overview of the field and covers the chemical, biological, mathematical and computational foundations of bioinformatics upon which later courses will depend. In addition, it introduces problems of interest to bioinformaticians and the methods and tools used to address them.

Prerequisite(s)/Corequisite(s): BIOI 1000 or BIOL 1450

BIOI 3000 APPLIED BIOINFORMATICS (3 credits)
This course will provide students with the practical skills needed for the analysis of -omics data. Topics covered will include biological databases, molecular biology tools (e.g., primer design, contig assembly), gene prediction and mining, database searches, genome comparison, sequence alignments, phylogenetic inference, gene expression data analyses, functional annotation of protein sequences, protein structure and modeling. Specialized software (e.g., Vector NTI) and widely used web-based computation tools (e.g., Entrez, BLAST, ClustalX, Phylip, PyMOL, and SwissPDBviewer) will be illustrated. Multiple approaches for solving particular problems will be presented.

Prerequisite(s)/Corequisite(s): BIOI 1000, BIOL 1450, and CIST 1400; or permission.

BIOI 3500 ADVANCED BIOINFORMATICS PROGRAMMING (3 credits)
Because of the volume and complexity of biological data, advanced programming skills are required for researchers in order to get the most out of their data analyses. This course will provide the expanded programming skills necessary to develop software that can exploit the complex information landscape of bioinformatics. Specific topics covered will include molecular biology basics, Unix/Linux shell programming, Perl and BioPerl, databases and using the Perl DBI, and data visualization.

Prerequisite(s)/Corequisite(s): BIOI 1000 and CSCI 1620. CSCI 3320 and an introductory course in biology (e.g., Biology 1450) are strongly recommended but not required.

BIOI 4500 INDEPENDENT STUDY (1-3 credits)
This course allows students to research a topic of their interest that is not available in a formal course. The topic to be studied must be agreed upon by the student and the instructor.

Prerequisite(s)/Corequisite(s): Junior or Senior within the Bioinformatics undergraduate program. Not open to non-degree graduate students.
BIOI 4510 BIOINFORMATICS INTERNSHIP (1-3 credits)
The purpose of this course is to provide the students with an opportunity for practical application and further development of knowledge and skills acquired in the Bioinformatics undergraduate program. The internship gives students professional work experience and exposure to the challenges and opportunities faced by IT professionals in the workplace.
Prerequisite(s)/Corequisite(s): Junior/Senior standing and permission of the Director of the School of Interdisciplinary Informatics. Not open to nondegree graduate students.

BIOI 4860 BIOINFORMATICS ALGORITHMS (3 credits)
The main objective of this course is to provide an organized forum for students to learn recent developments in Bioinformatics, particularly, from the algorithmic standpoint. The course will present basic algorithmic concepts in Bioinformatics and show how they are connected to molecular biology and biotechnology. Standard topics in the field such as restriction mapping, motif finding, sequence comparison, and database search will be covered. The course will also address problems related to Bioinformatics like next generation sequencing, DNA arrays, genome rearrangements and biological networks. (Cross-listed with BMI 8866).
Prerequisite(s)/Corequisite(s): CSCI 3320 and BIOL 1450; Or permission of instructor.

BIOI 4870 DATABASE SEARCH AND PATTERN DISCOVERY IN BIOINFORMATICS (3 credits)
This required course for undergraduate bioinformatics majors provides foundational knowledge on database aspects used in the field and an overview of their applications in bioinformatics, biomedical informatics, and health/clinical informatics. The course begins with a brief review of key concepts in computational molecular biology related to database search/development, database management systems, the difference between primary and secondary databases, and bioinformatics-related aspects of modeling and theory in computer science. The major focus is on the multiple challenges and aspects of bio-database development, search, and pattern discovery. The course uses problem-based learning to help students develop database management skills as they apply to high throughput ‘-omics.’ data, the basics of data management, data provenance and governance, standards, and analysis through KDD-based workflows. This course will also consider the fundamentals of artificial intelligence and machine learning as they pertain to bioinformatics, from the perspective of database storage, I/O, and analysis. (Cross-listed with CSCI 8876).
Prerequisite(s)/Corequisite(s): CSCI 4850 or permission of instructor. Not open to non-degree graduate students.

BIOI 4890 COMPUTERIZED GENETIC SEQUENCE ANALYSIS (3 credits)
The goal of this course is to introduce students to major topics in computerized analysis of genetic sequences. In particular the class will allow students to become familiar with the computational tools and software that aid in the modern molecular biology experiments and analysis of experimental results. Following the completion of this course, it is expected that the students will have a basic understanding of the theoretical foundations of the sequence analysis tools and develop competence in evaluating the output from these tools in a biological context. This course will emphasize hands-on experience with the programs for nucleotide and amino acid sequence analysis and molecular phylogeny.
Prerequisite(s)/Corequisite(s): Junior or senior-level standing in the Bioinformatics program or permission from the instructor. Not open to nondegree students.

BIOI 4950 SPECIAL TOPICS IN BIOINFORMATICS (3 credits)
This course is intended to provide a mechanism for offering instruction in subject areas that are not covered in other regularly scheduled courses. In general, courses offered under the BIOI 4950 designation will focus on evolving subject areas in bioinformatics.
Prerequisite(s)/Corequisite(s): Prerequisites of a specific offering of BIOI 4950 will be determined by the supervising faculty member and identified in the course proposal. It is anticipated that permission of the faculty member teaching the course will be required for registration.

BIOI 4970 SENIOR PROJECT IN BIOINFORMATICS I (1 credit)
This course is the first part of a two-part series that allows students to work on a guided research project on a specific topic in bioinformatics. The goal of this course is for the student to decide on a research topic and to write a detailed proposal based on this topic that outlines the goals and objectives of the proposed research. The topic and proposal will be approved by the supervising faculty member.
Prerequisite(s)/Corequisite(s): Senior level status in the Bioinformatics program. Not open to nondegree students.

BIOI 4980 SENIOR PROJECT IN BIOINFORMATICS II (2 credits)
This course is the second part of a two-part series that allows the student to work on a guided research project on a specific topic in bioinformatics. The goal of this course is for the student to perform the research proposed in Part I of the course and to present the results of his or her work. Presentations will be made in the form of a report, written as a scientific research paper, and an oral defense.
Prerequisite(s)/Corequisite(s): Senior-level standing in the Bioinformatics program and successful completion of BIOI 4970. Not open to nondegree students.

BIOI 4990 INDEPENDENT STUDY IN BIOINFORMATICS (1-3 credits)
This is a variable-credit course designed for the junior or senior bioinformatics major who would benefit from independent reading assignments and research-type problems. Independent study enables coverage of topics not taught in scheduled course offerings.
Prerequisite(s)/Corequisite(s): Junior/senior standing, permission of supervising faculty member & approval of Bioinformatics UG Prog Comm Chair. A formal description of the problem area to be investigated, the resources to be used, & the results to be produced must be prepared.

BIOI 8850 SPECIAL TOPICS IN BIOINFORMATICS (3 credits)
This course is intended to provide a mechanism for offering instruction in subject areas that are not covered in other regularly scheduled courses. In general, courses offered under the BIOI 8850 designation will focus on evolving subject areas in bioinformatics. The major focus is on the multiple challenges and aspects of bio-database development, search, and pattern discovery. The course uses problem-based learning to help students develop database management skills as they apply to high throughput ‘-omics.’ data, the basics of data management, data provenance and governance, standards, and analysis through KDD-based workflows. This course will also consider the fundamentals of artificial intelligence and machine learning as they pertain to bioinformatics, from the perspective of database storage, I/O, and analysis. (Cross-listed with CSCI 8876).
Prerequisite(s)/Corequisite(s): CSCI 4850 or permission of instructor. Not open to non-degree graduate students.

Cybersecurity

CYBR 1100 INTRODUCTION TO INFORMATION SECURITY (3 credits)
This course emphasizes our current dependence on information technology and how its security in cyberspace (or lack thereof) is shaping the global landscape. Several historical and contemporary global events that have been influenced by the exploitation of information technology motivates topics on cyber crime, malware, intrusion detection, cryptography, among others, and how to secure one's own data and computer system. Several aspects of this course are geared towards developing an understanding of the 'cyberspace' as a new medium that breaks all geographical boundaries, while highlighting noticeable influences on it from social, political, economic and cultural factors of a geographical region.
Distribution: Global Diversity General Education course

CYBR 2250 LOW-LEVEL PROGRAMMING (3 credits)
This course will teach the cybersecurity (CYBR) students low-level programming in the 'C' and assembly languages, and the interrelationship between these two programming paradigms. The student will learn the various control structures in 'C' and how they are implemented in machine code, memory allocation and management, and the basics of allocation classes such as static versus automatic variables. The students will also learn assembly language in the 'C' environment and will be able to write useful, functional, stand-alone assembly language programs with no help from external libraries.
Prerequisite(s)/Corequisite(s): CSCI 1620. Not open to non-degree graduate students.
CYBR 2980  SPECIAL TOPICS IN CYBERSECURITY (1-3 credits)
The course provides a format for exploring subject areas in Cybersecurity and related fields for sophomore undergraduate students. Specific topics vary, in keeping with research interests of faculty and students. Examples include network configuration, network security, forensics, regulatory compliance, web services and applications, vulnerability assessments, cloud computing security, and other issues in Cybersecurity.
Prerequisite(s)/Corequisite(s): Instructor permission required. Not open to non-degree graduate students.

CYBR 3250  SECURITY ADMINISTRATION - LINUX (3 credits)
This course covers topics a system administrator would encounter in their profession. The student will learn how a system administrator fulfills various organizational information resource management requirements using the a Linux-based Operating System. Topics will include; installation; creating and maintaining file systems; user and group administration; backup and restore processes; network configuration; various system services; simple security administration; and updating and maintaining the system.
Prerequisite(s)/Corequisite(s): CSCI 1620 or CSCI 1840 or Instructor Permission.

CYBR 3370  SECURITY ADMINISTRATION - WINDOWS (3 credits)
This course covers topics a system administrator would encounter in their profession. The student will learn how a system administrator fulfills various organizational information resource management requirements using the Windows Operating System. Topics will include; installation; creating and maintaining file systems; user and group administration; backup and restore processes; network configuration; various system services; simple security administration; and updating and maintaining the system.
Prerequisite(s)/Corequisite(s): CSCI 1620 or CSCI 1840 or Instructor Permission.

CYBR 3450  NATURAL LANGUAGE PROCESSING (3 credits)
The course will provide overview of the topics in natural language processing such as word and sentence tokenization, syntactic parsing, semantic role labeling, text classification. We will discuss fundamental algorithms and mathematical models for processing natural language, and how these can be used to solve practical problems. We will touch on such applications of natural language processing technology as information extraction and sentiment analysis. (Cross-listed with CSCI 3450).
Prerequisite(s)/Corequisite(s): Prereq: CSCI 2030 with C- or better; Co-req: CSCI 3320 with C- or better; Students should be comfortable w/ scripting (Python is the language extensively used in natural language processing tools including NLTK). Not open to non-degree graduate students.

CYBR 3570  CRYPTOGRAPHY (3 credits)
The course will provide a broad overview of the concepts, fundamental ideas, vocabulary, and literature base central to the study and development of cryptography and cryptanalysis. This course will explore historical development of cryptography, as well as methods used to defeat it. In addition, the course will cover the mathematical foundations of cryptography today, as well as some current uses of such cryptography, such as public key infrastructures, the Internet Key Exchange protocol, and more.
Prerequisite(s)/Corequisite(s): CSCI 3320 or ISQA 3300. Not open to non-degree graduate students.

CYBR 3600  INFORMATION SECURITY, POLICY AND AWARENESS (3 credits)
This course will cover the planning and development for information governance, security policies and procedures, and security awareness. (Cross-listed with CIST 3600)
Prerequisite(s)/Corequisite(s): CIST 2100; CIST 3110, which may be taken concurrently.

CYBR 4000  CENTER OF ACADEMIC EXCELLENCE-CYBER OPERATIONS COMPLETION CERTIFICATE (0 credits)
This course is utilized to provide a specific designation for students that have completed the Center of Academic Excellence - Cyber Operations coursework. It is a zero credit hour class used to designate the completion of this focus area in the cybersecurity curriculum.
Prerequisite(s)/Corequisite(s): Instructor Permission. The program committee will work w/ the UG advisors to verify that the student has fulfilled the requirements for this designation. If the student has fulfilled (or will soon) all the requirements, they may register for this class.

CYBR 4360  FOUNDATIONS OF CYBERSECURITY (3 credits)
Contemporary issues in computer security, including sources for computer security threats and appropriate reactions; basic encryption and decryption; secure encryption systems; program security, trusted operating systems; database security, network and distributed systems security, administering security; legal and ethical issues. (Cross-listed with CYBR 8366, CSCI 8366).
Prerequisite(s)/Corequisite(s): CSCI 3320 or CSCI 8325 OR ISQA 3400 OR By instructor permission.

CYBR 4380  DIGITAL FORENSICS (3 credits)
Digital forensics involves the preservation, identification, extraction, analysis and documentation of digital evidence stored on a variety of electronic devices. The aim of this course is to introduce students to acceptable approaches for collecting, analyzing and reporting data from a forensics investigation. Topics include: an introduction to digital forensics, data acquisition, first response, memory forensics, operating system forensics, and network forensics. Students will be required to perform several forensics analyses in a controlled lab environment, including acquiring forensically sound hard drive images, memory images and analyzing these using industry standard tools, such as Forensic Toolkit (FTK). The Digital Forensics class is designed for Cybersecurity, Computer Science and other qualified students to learn what actions are both appropriate and required for preserving, collecting and analyzing digital evidence in cases of intrusion, data theft or other cybercrimes. (Cross-listed with CSCI 4380)
Prerequisite(s)/Corequisite(s): The student must take the following before enrolling: CYBR 3600 or CIST 3600, CSCI 3550 or ISQA 3400, CYBR 3370, CYBR 3350. Alternatively, instructor permission can be sought for students who have not met all of the above requirements.

CYBR 4390  MOBILE DEVICE FORENSICS (3 credits)
Mobile device forensics is the science of recovering digital evidence from a mobile device under forensically sound conditions using accepted methods. The aim of this course is to introduce students to acceptable approaches for collecting, analyzing and reporting data from a mobile device forensics investigation. Topics include: an introduction to digital and mobile device forensics, mobile forensics standards, acquisition methods (manual, logical, physical and provider-side), Android and iOS filesystem analysis, decoding applications, application data analysis, and report writing. Students will be required to perform several investigations in a controlled lab environment, including acquiring forensically sound evidence and analyzing these using industry standard tools. (Cross-listed with CYBR 8396).
Prerequisite(s)/Corequisite(s): CYBR 4380/8386 - Computer and Network Forensics or Instructor's Permission.
CYBR 4430 QUANTUM COMPUTING AND CRYPTOGRAPHY (3 credits)
The course builds an understanding of exciting concepts behind quantum computing and quantum cryptography. In doing so it will introduce the principles of qubits, superposition, entanglement, teleportation, measurement, quantum error correction, quantum algorithms, quantum key exchange, quantum encryption, and secure quantum channels that are built using these principles. It will also discuss advantages of quantum computing and cryptography over classical computing and cryptography and limitations thereof. The students will come out with a working understanding of the field of quantum computing and quantum cryptography. During the course, students will also implement several of the quantum algorithms. (Cross-listed with CYBR 8436)
Prerequisite(s)/Corequisite(s): Co-requisites: CYBR 3570 or CSCI 4560; or Instructor permission.

CYBR 4440 INDUSTRIAL CONTROL SYSTEM SECURITY (3 credits)
The objective of this course is to research vulnerabilities into, and provide guidance for securing, industrial control systems (ICS). ICS is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system items such as Programmable Logic Controllers (PLC). The student will learn to identify network and device vulnerabilities and potential countermeasures to these weaknesses. (Cross-listed with CYBR 8446)
Prerequisite(s)/Corequisite(s): CSCI 3550.

CYBR 4450 HOST-BASED VULNERABILITY DISCOVERY (3 credits)
The class will cover security issues at an implementation and hardware level. The students will learn assembly language and the use of a reverse assembler and debugger. This will allow the student to analyze various ‘packing’ algorithms for computer viruses, the viruses themselves, operating system ‘hooking’, ‘fuzzing’, and other machine code, host-based exploits. The class will be using both Windows and Linux as operating systems. (Cross-listed with CYBR 8456.)
Prerequisite(s)/Corequisite(s): CSCI 3710 and CYBR 2250

CYBR 4460 NETWORK-BASED VULNERABILITY DISCOVERY (3 credits)
The course is an advanced class in which the students learn various techniques for testing for and identifying security flaws in network software and web applications. Internet technologies such as HTTP, DNS, DHCP, and others are examined in the context of cyber security. Students are expected to participate in numerous hands-on experiments related to Information Assurance with respect to web technologies. (Cross-listed with CYBR 8466)
Prerequisite(s)/Corequisite(s): CSCI 3550

CYBR 4450 COMPUTER SECURITY MANAGEMENT (3 credits)
The purpose of this course is to integrate concepts and techniques from security assessment, risk mitigation, disaster planning, and auditing to identify, understand, and propose solutions to problems of computer security and security administration. (Cross-listed with CIST 4540, CYBR 8546, ISQA 8546)
Prerequisite(s)/Corequisite(s): IASC 4360 or permission of the instructor.

CYBR 4580 CERTIFICATION AND ACCREDITATION OF SECURE SYSTEMS (CAPSTONE) (3 credits)
This is the BSIA capstone course where students extend and apply their knowledge in defining, implementing, and assessing secure information systems. Students will demonstrate their ability to specify, apply, and assess different types of countermeasures at different points in the enterprise with a special focus on system boundaries. Students will complete and defend a Certification and Accreditation package.
Prerequisite(s)/Corequisite(s): CIST 3600 or CYBR 3600; CIST 4360; CYBR 3350 or CYBR 3370; and CIST 4540 or CYBR 4540 may be taken prior to or concurrently. Not open to non-degree graduate students.

CYBR 4950 INTERNSHIP IN CYBERSECURITY (1-3 credits)
The course provides a format for a student to work with a local or national industry partner in a cyber-security oriented position, and to receive credit for this practical experience. The internship may or may not be a paid position, but will definitely be directly related to the Cybersecurity degree program. The class is proposed and organized by the student, with participating faculty supervising and input provided by the industry partner.
Prerequisite(s)/Corequisite(s): Instructor Permission.

CYBR 4980 SPECIAL TOPICS IN INFORMATION ASSURANCE (1-3 credits)
The course provides a format for exploring advanced research areas for undergraduate students in Information Assurance and related fields. Specific topics vary, in keeping with research interests of faculty and students. Examples include applied data mining, mobile security, web services and applications, vulnerability assessments, cloud computing security, and other issues in Information Assurance research. (Cross-listed with CYBR 8986)
Prerequisite(s)/Corequisite(s): Instructor Permission.

CYBR 4990 INDEPENDENT STUDY IN INFORMATION ASSURANCE (1-3 credits)
The course provides a format for exploring advanced research areas for undergraduate students in Information Assurance and related fields. The class is designed for students that would like to explore specific Information Assurance topics at a greater depth, or topics which are not currently a part of the IA curriculum. The class is proposed and organized by the student, with participating faculty mentoring.
Prerequisite(s)/Corequisite(s): Instructor Permission.

CYBR 8000 CENTER OF ACADEMIC EXCELLENCE-CYBER OPERATIONS COMPLETION CERTIFICATE (0 credits)
This course is utilized to provide a specific designation for students that have completed the Center of Academic Excellence - Cyber Operations coursework. It is a zero credit hour class used to designate the completion of this focus area in the cybersecurity curriculum.
Prerequisite(s)/Corequisite(s): Instructor Permission. The program committee will work with the UG advisors to ascertain that the student has fulfilled all requirements for this designation. If he/she has or will within the last semester, they will be allowed to register for this class.

CYBR 8080 SPECIAL TOPICS IN INFORMATION ASSURANCE (1-6 credits)
The course provides a format for exploring advanced research areas for graduate students in Information Assurance and related fields. Specific topics vary, in keeping with research interests of faculty and students. Examples include applied data mining, mobile security, web services and applications, vulnerability assessments, cloud computing security, and other issues in Information Assurance research.
Prerequisite(s)/Corequisite(s): Instructor Permission.

CYBR 8366 FOUNDATIONS OF CYBERSECURITY (3 credits)
Contemporary issues in computer security, including sources for computer security threats and appropriate reactions; basic encryption and decryption; secure encryption systems; program security, trusted operating systems; database security, network and distributed systems security, administering security; legal and ethical issues. (Cross-listed with CYBR 4360, CSCI 8366)
Prerequisite(s)/Corequisite(s): CSCI 3320 or CSCI 8325 OR ISQA 3400 OR By instructor permission.
Cryptography. During the course, students will also implement several of the principles of qubits, superposition, entanglement, teleportation, measurement, quantum error correction, quantum algorithms, quantum key exchange, quantum encryption, and secure quantum channels that are built using these principles. It will also discuss advantages of quantum computing and cryptography over classical computing and quantum cryptography. During the course, students will also implement several of the quantum algorithms. (Cross-listed with CYBR 4430)

CYBR 8386 COMMERCE AND NETWORK FORENSICS (3 credits)
Computer forensics involves the preservation, identification, extraction and documentation of computer evidence stored on a computer. This course takes a technical, legal, and practical approach to the study and practice of incident response, computer forensics, and network forensics. Topics include legal and ethical implications, duplication and data recovery, steganography, network forensics, and tools and techniques for investigating computer intrusions. This course is intended as a second course in information assurance for undergraduate students as well as other qualified students. It is also intended as a foundation course for graduate digital forensics studies.

Prerequisite(s)/Corequisite(s): CYBR 1100, CIST 3600, CSCI 3500 or ISQA 3400, CYBR 3350 or CYBR 3370; or instructor permission.

CYBR 8396 MOBILE DEVICE FORENSICS (3 credits)
Mobile device forensics is the science of recovering digital evidence from a mobile device under forensically sound conditions using accepted methods. The aim of this course is to introduce students to acceptable approaches for collecting, analyzing and reporting data from a mobile device forensics investigation. Topics include: an introduction to digital and mobile device forensics, mobile forensics standards, acquisition methods (manual, logical, physical and provider-side), Android and iOS filesystem analysis, decoding approaches, application data analysis, and report writing. Students will be required to perform several investigations in a controlled lab environment, including acquiring forensically sound evidence and analyzing these using industry standard tools. (Cross-listed with CYBR 4390).

CYBR 8410 DISTRIBUTED SYSTEMS AND NETWORK SECURITY (3 credits)
The course aims at understanding the issues surrounding data security, integrity, confidentiality and availability in distributed systems. Further, we will discuss various network security issues, threats that exist and strategies to mitigate them. This course will cover topics in cryptography, public key infrastructure, authentication, hashing, digital signatures, ARP protection, IP and IPSEC, IP Tables, SSL/TLS, firewalls, etc. (Cross-listed with CSCI 8410)

Prerequisite(s)/Corequisite(s): IASC 8366 or equivalent(s); or instructor permission. Not open to non-degree graduate students.

CYBR 8420 SOFTWARE ASSURANCE (3 credits)
Software assurance is a reasoned, auditable argument created to support the belief that the software will operate as expected. This course is an intersection of knowledge areas necessary to perform engineering activities or aspects of activities relevant for promoting software assurance. This course takes on a software development lifecycle perspective for the prevention of flaws. (Cross-listed with CSCI 8420)

Prerequisite(s)/Corequisite(s): CSCI 4830 or CSCI 8836 OR by permission of the Instructor. Not open to non-degree graduate students.

CYBR 8436 QUANTUM COMPUTING AND CRYPTOGRAPHY (3 credits)
The course builds an understanding of existing concepts behind quantum computing and quantum cryptography. In doing so it will introduce the principles of qubits, superposition, entanglement, teleportation, measurement, quantum error correction, quantum algorithms, quantum key exchange, quantum encryption, and secure quantum channels that are built using these principles. It will also discuss advantages of quantum computing and cryptography over classical computing and cryptography and limitations thereof. The students will come out with a working understanding of the field of quantum computing and quantum cryptography. During the course, students will also implement several of the quantum algorithms. (Cross-listed with CYBR 4430)

CYBR 8440 SECURE SYSTEMS ENGINEERING (3 credits)
This course takes a global risk-based view of the process of defining, verifying, validating and continuously monitoring secure information systems. The course will investigate a number of secure system solutions, starting with the definition of the system security needs, and tracing through methods of verification and validation of security controls, as well as ways to continuously monitor the corresponding assurances. (Cross-listed with CSCI 8440)

Prerequisite(s)/Corequisite(s): CSCI 8366 or IASC 8366.

CYBR 8446 INDUSTRIAL CONTROL SYSTEM SECURITY (3 credits)
The objective of this course is to research vulnerabilities into, and provide guidance for securing, industrial control systems (ICS). ICS is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system items such as Programmable Logic Controllers (PLC). The student will learn to identify network and device vulnerabilities and potential countermeasures to these weaknesses. (Cross-listed with CYBR 4440)

Prerequisite(s)/Corequisite(s): CSCI 8410 or CYBR 8410

CYBR 8450 APPLIED CRYPTOGRAPHY (3 credits)
In this course we will implement stream and block ciphers in different modes, public key algorithms, hash functions, message authentication codes, random number generators, etc. Along the way we will also explore weaknesses of these algorithms and implement well-known attacks on them. We will also solve crypto challenges and puzzles. This is a hand-on course and will require programming proficiency. The preferred language will be Python; you can, however, use other object oriented languages.

Prerequisite(s)/Corequisite(s): CSCI 8410 or CYBR 8410

CYBR 8456 HOST-BASED VULNERABILITY DISCOVERY (3 credits)
The class will cover security issues at an implementation and hardware level. The students will learn assembly language and the use of a reverse assembler and debugger. This will allow the student to analyze various ‘packing’ algorithms for computer viruses, the viruses themselves, operating system ‘hooking’, ‘fuzzing’, and other machine code, host-based exploits. The class will be using both Windows and Linux as operating systems. (Cross-listed with CYBR 4450.)

Prerequisite(s)/Corequisite(s): CSCI 8410 or CYBR 8410

CYBR 8466 NETWORK-BASED VULNERABILITY DISCOVERY (3 credits)
The class will cover security issues at an implementation and hardware level. The students will learn assembly language and the use of a reverse assembler and debugger. This will allow the student to analyze various ‘packing’ algorithms for computer viruses, the viruses themselves, operating system ‘hooking’, ‘fuzzing’, and other machine code, host-based exploits. The class will be using both Windows and Linux as operating systems. (Cross-listed with CYBR 4460)

Prerequisite(s)/Corequisite(s): CSCI 3710 and CYBR 2250.

CYBR 8466 NETWORK-BASED VULNERABILITY DISCOVERY (3 credits)
The course is an advanced class in which the students learn various techniques for testing for and identifying security flaws in network software and web applications. Internet technologies such as HTTP, DNS, DHCP, and others are examined in the context of cyber security. Students are expected to participate in numerous hands-on experiments related to Information Assurance with respect to web technologies. (Cross-listed with CYBR 4460)

Prerequisite(s)/Corequisite(s): CSCI 3710

CYBR 8470 SECURE WEB APPLICATION DEVELOPMENT (3 credits)
Web applications are pervasive fixtures of 21st century culture. Web application security is an inclusive, amorphous, term that spans application level security, i.e. ensuring high level code cannot be exploited, server level security, i.e. ensuring server resources such as databases and file systems cannot be exploited, and network security, i.e. ensuring unauthorized parties cannot access a server or tamper with user sessions. This course cross-cuts the web application security concepts across the different categories above and takes a heavily hands-on approach to introduce students to the world of secure web app. design and development.

Prerequisite(s)/Corequisite(s): Instructor Permission
**CYBR 8480 SECURE MOBILE DEVELOPMENT (3 credits)**
Mobile devices are already pervasive fixtures of 21st century culture and increasingly the internet of things (IoT) and wearables are proliferating throughout the world. As this proliferation occurs, numerous vendor-centric and third-party mobile, wearable, and internet of things apps are being created by developers and downloaded by end-users with little to no thought about the security and privacy of the information used and collected by the apps. This course examines this issue from a development point of view to a) introduce mobile wearable/IoT architectures and technologies, b) increase student application development competencies with these technologies, and c) integrate secure design principles into the ideation, design, and testing phases during development.

**Prerequisite(s)/Corequisite(s):** CYBR 8470 or Instructor Permission

**CYBR 8546 COMPUTER SECURITY MANAGEMENT (3 credits)**
The purpose of this course is to integrate concepts and techniques from security assessment, risk mitigation, disaster planning, and auditing to identify, understand, and propose solutions to problems of computer security and security administration. (Cross-listed with CIST 4540, CYBR 4540, ISQA 8546)

**Prerequisite(s)/Corequisite(s):** IASC 4360 or permission of the instructor.

**CYBR 8570 INFORMATION SECURITY POLICY AND ETHICS (3 credits)**
The course will cover the development and need for information security policies, issues regarding privacy, and the application of computer ethics. (Cross-listed with ISQA 8570)

**Prerequisite(s)/Corequisite(s):** CIST 2100 or BSAD 8030, or permission of instructor.

**CYBR 8900 INDEPENDENT STUDY IN INFORMATION ASSURANCE (1-3 credits)**
The course provides a format for exploring advanced research areas for graduate students in Information Assurance and related fields. The class is designed for students that would like to explore specific Information Assurance topics at a greater depth, or topics that are not currently a part of the IA curriculum. The class is proposed and organized by the student, with participating faculty mentoring.

**Prerequisite(s)/Corequisite(s):** Instructor Permission

**CYBR 8910 INTERNSHIP (1-3 credits)**
The purpose of this course is to provide the students with an opportunity for practical application and further development of knowledge and skills acquired in the MS in CyberSecurity (CYBR) program. The internship gives students professional work experience and exposure to the challenges and opportunities faced by IT professionals in the workplace.

**Prerequisite(s)/Corequisite(s):** Students must have completed a minimum of 12 credit hours towards the MS in CYBR program. Instructor permission is required to register. Not open to non-degree graduate students.

**CYBR 8950 GRADUATE CAPSTONE IN INFORMATION ASSURANCE (3 credits)**
This is the graduate capstone course where students extend and apply their knowledge in defining, implementing, and assessing secure information systems. Students will demonstrate their ability to specify, apply, and assess different types of countermeasures at different points in the enterprise with a special focus on system boundaries. Students will complete and defend a Certification and Accreditation package. This course is intended for graduate students in the MS in IA degree program, coursework option, that are close to graduation (see prerequisites). This course replaces the MS in IA comprehensive examination requirement.

**Prerequisite(s)/Corequisite(s):** CYBR 8366, CYBR 8410, and CYBR 8456 and concentration area (systems or management and policy). Students must have 6 credit hours or less left in the program.

**CYBR 8986 SPECIAL TOPICS IN INFORMATION ASSURANCE (1-3 credits)**
The course provides a format for exploring advanced research areas for undergraduate students in Information Assurance and related fields. Specific topics vary, in keeping with research interests of faculty and students. Examples include applied data mining, mobile security, web services and applications, vulnerability assessments, cloud computing security, and other issues in Information Assurance research. (Cross-listed with CYBR 4980)

**Prerequisite(s)/Corequisite(s):** Instructor Permission.

**CYBR 8990 THESIS IN INFORMATION ASSURANCE (1-6 credits)**
A research project, designed and executed under the supervision of the chair and approval by members of the graduate student's thesis advisory committee. In this project the student will develop and perfect a number of skills including the ability to design, conduct, analyze and report the results in writing (i.e., thesis) of an original, independent scientific investigation.

**Prerequisite(s)/Corequisite(s):** Instructor Permission.

**CYBR 9460 SECURITY OF EMBEDDED SYSTEMS (3 credits)**
An embedded system is some combination of computer hardware and software, either fixed in capability or programmable, which is specifically designed for a particular function. Industrial machines, automobile electronic systems, medical equipment, cameras, household appliances, airplanes, and vending machines, are among the myriad possible hosts of an embedded system. This course covers forward-looking topics in the security of embedded systems, including topics such as logic circuit obfuscation, hardware security methods, network setup exploits, and other 'lower level' computer architecture subjects with respect to cybersecurity.

**Prerequisite(s)/Corequisite(s):** CYBR 8366 - Foundations of Information Assurance

**IT Innovation**

**ITIN 1010 ACTIVATING INNOVATION IN SOCIETY (3 credits)**
This course surveys and applies the use of qualitative methods, especially interview-based research, in order to maximize the insight that informs and activates the innovation process, with emphasis on technological innovation.

**Prerequisite(s)/Corequisite(s):** Not open to non-degree graduate students.

**Distribution:** Social Science General Education course

**ITIN 1110 INTRODUCTION TO IT INNOVATION (3 credits)**
In almost every modern human endeavor, creativity and Information Technology are essential. In the Internet age, information has become a commodity that is available to everyone. Similarly, current technology has largely become commoditized. Therefore, creating new value is becoming the basis for successful professionals. This course introduces students to tools, techniques, and methods for generating innovative information technology ideas and solutions. It teaches them to think about future possibilities and equips them with the ability to critically evaluate proposed innovations and ideas. The goal of the course is to increase students' ability to creatively solve challenging problems in new ways using information technology. This class is inherently interdisciplinary as IT now touches every aspect of modern academic pursuits.

**Prerequisite(s)/Corequisite(s):** Not open to non-degree graduate students.

**ITIN 2150 AUDIO FOR MULTIMEDIA (3 credits)**
This course provides an overview of audio production techniques as they pertain to multimedia.

**Prerequisite(s)/Corequisite(s):** Not open to non-degree graduate students.
ITIN 2220 APPLIED IT INNOVATION (3 credits)
The course extends the concepts learned in the Introduction to IT Innovation course and focuses on market dynamics and monetizing innovations. It moves past idea generation and focuses on identifying and gathering resources, innovation implementation, sustainable innovation models and how ideas can be monetized. The goal is for students to take their original ideas from concept to initial implementation with thoughts towards commercialization. Upon completing the course, students will have created at least a rudimentary implementation of an original idea and have a defensible plan for how the idea can be monetized.
Prerequisite(s)/Corequisite(s): ITIN 1110 & CIST 1400. Not open to non-degree graduate students.

ITIN 2990 IT INNOVATION SYMPOSIUM (1 credit)
The seminar exposes students to information technology innovators from multiple industries and varied backgrounds. It teaches the practical aspects of IT Innovation from those that have done it and are doing it in both research and practice. The purpose is to cause students to reflect on applying innovation to the real-world, connect them to the innovation community and to equip them with best practices and tools to make their innovations a reality.
Prerequisite(s)/Corequisite(s): Enrollment in the IT Innovation Major or IT Innovation Minor. Not open to non-degree graduate students.

ITIN 3100 MUSIC INFORMATICS (3 credits)
Surveys the use of digital music data in the study, composition, performance, analysis, storage, and dissemination of music. Various computational approaches and technologies in music informatics including music information retrieval will be explored and implemented by students. (Cross-listed with MUS 3100).
Prerequisite(s)/Corequisite(s): Successful completion of one of the following three courses satisfies the prerequisite requirement: CIST 1300 or MUS 3170 or MUS 3180. Not open to non-degree graduate students.

ITIN 3180 DIGITAL SYNTHESIS (3 credits)
An exploration of the potentials of computer music synthesis. Concepts of music synthesis are presented through the use of a computer, keyboard, and appropriate software. Students create assignments that demonstrate the application of basic techniques. (Cross-listed with MUS 3180).

ITIN 3330 PRODUCT DESIGN AND DEVELOPMENT (3 credits)
This course will cover elements and principles of excellent product design and development. The history of design will be reviewed and overarching tenets of design will be introduced. The course will particularly focus on innovation and students will be expected to develop an original concept and create quality designs and low-fidelity prototype implementations of their unique idea. The proposed solutions must be novel and meet a real-world market need. This course will be hands-on and will examine developmental models for innovation.
Prerequisite(s)/Corequisite(s): ITIN 2220. Not open to non-degree graduate students.

ITIN 4000 SPECIAL TOPICS IN IT INNOVATION (1-6 credits)
This course is designed to acquaint students with issues which are current to the field or emerging trends in the IT Innovation area. Topics will vary across terms. This course may be repeated, but no topic may be taken more than once. (Cross-listed with ITIN 8006).
Prerequisite(s)/Corequisite(s): Permission of instructor. Additional prerequisites may be required for particular topic offerings.

ITIN 4090 PRINCIPLES OF COLLABORATION (3 credits)
Students will work with techniques for team leadership, interpersonal collaboration, consensus-building, creative problem solving, negotiation, facilitation, group process design, collaborative workspace design, and collaboration engineering. Students will gain hands-on experience with collaboration technologies. (Cross-listed with BSAD 8096, MGMT 4090).
Prerequisite(s)/Corequisite(s): Junior standing or permission of instructor.

ITIN 4260 USER EXPERIENCE DESIGN (3 credits)
User experience (UX) design is concerned with the application of user-centered design principles to the creation of computer interfaces ranging from traditional desktop and web-based applications, mobile and embedded interfaces, and ubiquitous computing. This course provides in-depth, hands-on experience with real world application of the iterative user-centered process including contextual inquiry, task analysis, design ideation, rapid prototyping, interface evaluation, and reporting usability findings. (Cross-listed with CSCI 4260, CSCI 8266, ITIN 8266).
Prerequisite(s)/Corequisite(s): Required: C- or better in CIST 2500 and junior standing, or by permission of instructor. Recommended: C- or better in CSCI 4250 or ITIN 3330.

ITIN 4440 AGILE DEVELOPMENT METHODS (3 credits)
The course presents an introduction to agile development methods for IT application development. Students will also learn Unified Modeling Techniques as they go through the agile iterations. This course is a foundation course for the IT Innovation capstone course.
Prerequisite(s)/Corequisite(s): CSCI 4850 or ISQA 3310. Not open to non-degree graduate students.

ITIN 4500 INDEPENDENT STUDIES (1-3 credits)
A variable credit course for the junior or senior who will benefit from independent reading assignments and research type problems. Independent study makes available courses of study not available in scheduled course offerings. The student wishing to take an independent study course should find a faculty member willing to supervise the course and then submit, for approval, a written proposal (including amount of credit) to the IT Innovation Undergraduate Program Committee at least three weeks prior to registration.
Prerequisite(s)/Corequisite(s): Written permission required.

ITIN 4510 INFORMATION TECHNOLOGY INNOVATION INTERNSHIP (1-3 credits)
The purpose of this course is to provide the students with an opportunity for practical application and further development of knowledge and skills acquired in the IT Innovation undergraduate program. The internship gives students professional work experience and exposure to the challenges and opportunities faced by professionals in the workplace.
Prerequisite(s)/Corequisite(s): Junior/Senior standing and permission of School of interdisciplinary Informatics Director. Not open to non-degree graduate students.

ITIN 4720 INNOVATION VENTURES (3 credits)
This team-based course provides students with the opportunity to practice the basic tools of business discovery and validation, both as an instrument for new venture formation and as a core capability for addressing challenges in competitive landscapes. As such, the course lies at the intersection of innovation, entrepreneurship and strategy. Students will develop practical experience by experimenting with and refining business ideas. (Cross-listed with BSAD 8726, ENTR 4720, ITIN 8256, MGMT 4720, MKT 4720).
Prerequisite(s)/Corequisite(s): ITIN 1110 and junior standing or above or by instructor permission.

ITIN 4880 SYSTEMS SIMULATION AND MODELING (3 credits)
The course provides an introduction to the modeling and simulation with special emphasis on decision-theoretic models and rational decision-making. The ability to make good decisions is key to individuals and organizations and studying, understanding and improving decisions is vital to success. Students are given a background into systematic decision-making processes, and then are introduced to formal methods for decision modeling and analysis. Building on these foundational models, students learn how to perform process modeling and optimization. Finally, the course concludes with a look at psychological biases and traps that may affect decision-makers. (Cross-listed with ISQA 4880).
Prerequisite(s)/Corequisite(s): CIST 1400, CIST 2500, or equivalent.
ITIN 4980 INFORMATION TECHNOLOGY INNOVATION CAPSTONE PROJECT I (3 credits)
This course serves as Part 1 of the capstone project for the Information Technology Innovation program. As such the student will design a prototype of an IT product or service as well as a business case pertaining to what is required to launch their project commercially. This effort will be under the guidance of an advisory committee.
Prerequisite(s)/Corequisite(s): ITIN 4440. ITIN 4980 is for seniors who are enrolled in the BS in IT innovation degree. Before enrolling in ITIN 4980, a student must gain approval, from the ITIN Program Committee, of their Area of Emphasis. Not open to non-degree graduate students.

ITIN 4990 INFORMATION TECHNOLOGY INNOVATION CAPSTONE PROJECT PART II (3 credits)
This course serves as Part 2 of the capstone project for the Information Technology Innovation program. Following the designs and business plan developed in Part I ITIN 4980, the student will create a prototype of an IT product or service as well as refine and implement the required business aspects involved in launching their project commercially. This effort will be under the guidance of an advisory committee.
Prerequisite(s)/Corequisite(s): ITIN 4980. This course is for seniors who are enrolled in the BS in IT Innovation degree. Not open to non-degree graduate students.

ITIN 8000 TECHNOLOGY & INNOVATION-STATE OF THE ART (0 credits)
ITIN 8000 provides a regular forum for IT Innovation graduates students, where the latest developments in the field of IT Innovation are introduced and discussed. The course also functions as a central communication and collaboration hub for graduate students in IT Innovation. Participation is required.
Prerequisite(s)/Corequisite(s): Students in the MS in IT Innovation program may register. Not open to non-degree graduate students.

ITIN 8006 SPECIAL TOPICS IN IT INNOVATION (1-6 credits)
This course is designed to acquaint students with issues which are current to the field or emerging trends in the IT Innovation area. Topics will vary across terms. This course may be repeated, but no topic may be taken more than once. (Cross-listed with ITIN 4000).
Prerequisite(s)/Corequisite(s): Permission of instructor. Additional prerequisites may be required for particular topic offerings.

ITIN 8100 INTERMEDIA (3 credits)
This is an ongoing course that brings together students of the arts and students of scientific disciplines in order to facilitate and promote the creation of intermedia art, and to further explore shared resources, joint research, and exhibition/performance opportunities.
Prerequisite(s)/Corequisite(s): Instructor permission

ITIN 8210 DESIGN SCIENCE AND THEORY DEVELOPMENT (3 credits)
The purpose of this course is to help students understand theory, theoretical contributions, and design science. Students will approach such questions as: What is a theory? What makes a good theory? Why are theories just theories and not laws? What is not a theory? Following this introduction, we explore design science as a research methodology and Information Technology design theories. Ultimately, students create their own new studies around some design concept.
Prerequisite(s)/Corequisite(s): Graduate standing / permission of the instructor

ITIN 8220 DESIGN PROCESS (3 credits)
Inter-disciplinary design teams will work together to design and innovate products of the future. The design projects in the course are developed to directly address a problem brought forward by a technology company in the Omaha area in order to provide students with a design experience that directly impacts real-world product development. Students will focus on the technological (interface), physical (ergonomics) and aesthetic quality of design, and will learn how to conduct rigorous user studies in a laboratory setting. Teams will be cross disciplinary and consider all aspects of the design, creation, testing, and fabrication of the products.

ITIN 8256 INNOVATION VENTURES (3 credits)
This team-based course provides students with the opportunity to practice the basic tools of business discovery and validation, both as an instrument for new venture formation and as a core capability for addressing challenges in competitive landscapes. As such, the course lies at the intersection of innovation, entrepreneurship and strategy. Students will develop practical experience by experimenting with and refining business ideas. (Cross-listed with BSAD 8726, ENTR 4720, ITIN 4720, MGMT 4720, MKT 4720).
Prerequisite(s)/Corequisite(s): Admission to a graduate program or instructor permission.

ITIN 8266 USER EXPERIENCE DESIGN (3 credits)
User experience (UX) design is concerned with the application of user-centered design principles to the creation of computer interfaces ranging from traditional desktop and web-based applications, mobile and embedded interfaces, and ubiquitous computing. This course provides in-depth, hands-on experience with real world application of the iterative user-centered process including contextual inquiry, task analysis, design ideation, rapid prototyping, interface evaluation, and reporting usability findings. (Cross-listed with CSCI 4260, CSCI 8266, ITIN 4260).

ITIN 8300 RESEARCH FOUNDATIONS (3 credits)
This course serves as an introduction to research literature and research methodology in the innovation and creativity research domain. Students are introduced to skills, methodological issues, and bibliographic resources to enhance their ability in critically evaluating and conducting research in the IT Innovation field. Through a series of readings, in-class discussions, and lectures the student will select and define a research question, explore the various types of research designs and complete a literature review. This course is structured to make research meaningful and significant and enable students to write effectively.
Prerequisite(s)/Corequisite(s): ITIN 8900 or equivalent

ITIN 8900 INDEPENDENT STUDIES (1-3 credits)
A variable credit course for the graduate student who will benefit from independent reading assignments and research type problems. Independent study makes available courses of study not available in scheduled course offerings. The student wishing to take an independent study course should find a faculty member willing to supervise the course and then submit, for approval, a written proposal (including amount of credit) to the IT Innovation Graduate Program Committee Chair at least three weeks prior to registration.
Prerequisite(s)/Corequisite(s): Written permission required

ITIN 8940 INFORMATION TECHNOLOGY INNOVATION CAPSTONE I (3 credits)
The purpose of the Information Technology Innovation (ITIN) capstone courses is for ITIN majors to explore, identify, evaluate, design, construct and implement a new innovative product that leverages information technology and includes an interdisciplinary field of study. The capstone is the culmination product of the specific various disciplines a student has selected as the unique combination for his or her degree. This course serves as part one of the capstone project for the ITIN Masters degree. The two courses for the ITIN capstone project are intended to be completed in two consecutive semesters (Fall/Spring).
Prerequisite(s)/Corequisite(s): Must be pursuing ITIN MS degree and have completed: two sections of ITIN 8000, ITIN 8220, 8300, and 3 hours of upper division courses in interdisciplinary area identified in the student’s course plan. Not open to non-degree graduate students.
ITIN 8950 ITIN CAPSTONE II (3 credits)
The purpose of the ITIN capstone courses is for ITIN majors to explore, identify, evaluate, design, construct and implement a new innovative product that leverages information technology and an interdisciplinary field. The capstone is the culmination product for prospective graduate and utilizes the discipline(s) a student has selected as the unique combination for his or her degree. This course serves as part two of the capstone project for the Information Technology Innovation (ITIN) program. The two courses for the ITIN capstone project are taught in two consecutive semesters.
**Prerequisite(s)/Corequisite(s):** Must be pursuing ITIN MS degree and have completed: three sections of ITIN 8000, ITIN 8220, 8300, 8940 and 6 hours of upper division courses in interdisciplinary area identified in the student’s course plan. Not open to non-degree graduate students.

ITIN 8990 THESIS (1-6 credits)
This course is required for the Master of Science degree in the MS in IT Innovation Program. The purpose of this course is to conduct original research in IT Innovation, under supervision of a faculty member, culminating in a paper document that represents the student’s competency in their chosen field, as well as scholarly contributions. With consultation from their committee, MS in IT Innovation thesis students should be prepared to independently complete the writing of their thesis and successfully defend their thesis.
**Prerequisite(s)/Corequisite(s):** Graduate major in ITIN and approval of the Thesis Advisory Committee.

ITIN 9300 SOCIAL COMPUTING AND ITS APPLICATIONS (3 credits)
It is indisputable that social media and the Internet more broadly reshaped information disbursement and processing. Digital participation and communication has become the ‘new normal’ and the dividing line between off- and online communities is increasingly blurred. This leads to specific challenges in the extraction and analysis of online social media data, and the management of new communication.
**Prerequisite(s)/Corequisite(s):** Open to all currently-admitted doctoral students. Students should have a technical aptitude; experience with at least one web scripting language, (e.g. PHP, rails, python etc) is helpful. Experience with JSON is advantageous but not essential.