Illinois Institute of Technology  
National Center of Academic Excellence in Information Assurance/Cyber Defense Education  

National Center of Academic Excellence in Information Assurance/Cyber Defense Education  

National Center of Academic Excellence in Information Assurance/Cyber Defense in Education Four-year+ (CAE IA/CD) 

These criteria are applicable to regionally accredited four-year colleges, graduate-level universities, and DoD schools. 

Criteria for this designation include: 

- Demonstration of program outreach and collaboration, student development, IA/CD Center establishment and maintenance, IA/CD multidisciplinary efforts, practice of IA/CD at the institution level, IA/CD faculty, and student curriculum path and recognition; 
- Successful mapping of the institution’s curriculum to all of the two-year Core Knowledge Units (KUs), the four-year Core KUs, and five (5) Optional KUs of the institution’s choice. 

CAE IA/CD Program requirements 

1. Outreach/Collaboration. The institution must demonstrate how IA/CD is extended beyond the normal boundaries of the Institution. 

**Overall Point Value: 15 points minimum/25 points maximum** 

a. Shared curriculum (e.g., IA/CD teaching materials provided to minority colleges/universities, two-year community colleges, technical schools, or K-12 schools) or shared faculty (e.g., Faculty on IA/CD curriculum development committee and/or teaching IA/CD at minority colleges and universities, two-year community colleges, technical schools, or K-12 schools.) 

**Point Value: Up to 5 points/3 points required** 

Industry Professor of Information Technology and Management Ray Trygstad serves on the Advisory Committees for both the Computer Information Systems and Computer Internetworking Technology curricula at College of DuPage, Glen Ellyn, Illinois. Professor Trygstad and Industry Associate Professor of Information Technology and Management Jeremy Hajek serve on the Advisory Committee for the Computer Information Systems curriculum at Triton College, River Grove, Illinois. They actively advise chairs and coordinators at these institutions on cyber security and forensics courses and curricula. 

Two IIT adjunct faculty members, also Members of the IIT Center for Cyber Security and Forensics Education (C²SAFE), are full-time faculty members at local community colleges. Adjunct Industry Associate Professor of Information Technology and Management Sheikh ‘Sam’ Shamsuddin is an Assistant Professor of Computer Information Systems and Computer Internetworking Technology (joint appointment), at the College of DuPage, Glen Ellyn, Illinois where he teaches digital forensics and operating system courses. Adjunct Industry Associate Professor of Information Technology and Management Kevin Vaccaro is an Instructor of Cybersecurity at Moraine Valley Community College, Palos Hills, Illinois, where he teaches a broad variety of courses in cyber security.
b. Reciprocity of credits (e.g., Accepting academic credit in IA/CD courses from minority institutions, two-year community colleges, or technical schools.). Evidence in the form of written agreements must demonstrate that IA/CD-related courses from the above types of schools are accepted for credit at the applying institution.

**Point Value: Up to 5 points/3 points required**


In addition, a defined Guided Pathway to Success (GPS) into IIT's Information Technology and Management curriculum has been drafted jointly by Chicago City Colleges and IIT. The draft can be viewed at http://dickens.rice.iit.edu/CAEIA/CityColleges-IIT_ITM_pathway.pdf. This pathway is expected to be formally published for use by by City College students within the next month.

c. Sponsorship of or participation in Cyber Defense or Forensics Exercises and competitions within 3 years of submission. Sponsorship of state, regional, or national IA/CD curriculum workshops, colloquia, etc. (e.g., sponsorship of workshops for K-12, community colleges, technical schools, state homeland security, industry, etc.)

**Point Value: Up to 5 points**

The IIT School of Applied Technology has sponsored ForenSecure, a regional conference on cyber security and digital forensics, for the last 12 years. As a part of the annual ForenSecure conference, we sponsored and conducted the Malware Challenge in 2013 (http://forensecure.sat.iit.edu/2013/content/session-abstracts) and a more complex Security Challenge in 2014 (http://forensecure.sat.iit.edu/2014/challenge); both were designed and conducted by center member Shawn Davis.

In addition, in conjunction with the 2013 ForenSecure conference, our student organization, ITMO, co-sponsored a Hacking Challenge with IIT and Barrier1, with a $1000 prize for the winning team (http://mypages.iit.edu/~itmo/hackthis/).

ITM student Eric Tendian competed in the Cyber Aces State Championship offered by the Illinois Department of Employment Security (IDES) and placed second of 125 participants, many of whom were professionals in the field. (http://blogs.iit.edu/itm_loopback/2014/03/06/iit-itm-student-wins-2nd-place-in-cyber-aces-state-championship/)

d. CAE Collaboration. Partner in research/shared classes or shared events with other institutions. Institutions are encouraged to partner with other CAEs on cyber or IA/CD research/instruction.

**Point Value: Up to 5 points**

IIT is a member of the Center for Systems Security and Information Assurance, a National Science Foundation (NSF) Advanced Technological Education (ATE)
National Resource Center (http://www.cssia.org/) located in Palos Hills, Illinois. (http://www.cssia.org/cssia-affiliates-display.cfm?id=340) In addition, faculty, staff, and students from colleges and universities throughout the region actively participate in ForenSecure, our regional conference on cyber security and digital forensics; see more details on this conference in the following paragraph.

e. Community Outreach. Sponsorship of community events such as cybersecurity education for local schools, adult education centers, senior centers, etc. (e.g., schools in a target region are encouraged to participate in cybersecurity education events, like community computer diagnostic “check-ups” and IA/CD awareness days.)

Point Value: Up to 5 points

The IIT School of Applied Technology has sponsored ForenSecure, a regional conference and expo on cyber security and digital forensics, for the last 12 years. Upon creation of the IIT Center for Cyber Security and Forensics Education in 2012, the conference became a formal activity of the Center. This conference brings together business professionals, business and industry security practitioners, government and law enforcement, industry sponsors, faculty, and students for two days of presentations in three tracks. These tracks feature discussion and debate over issues related to ethical hacking, security, digital forensics, policy and compliance, cyberterrorism, privacy, cloud computing, and more. A truly regional conference, attendees come from Iowa, Indiana, and Michigan, as well as the greater Chicago area. Student presentations represent an opportunity for the best students in our Cyber Security and Forensics curricula to demonstrate their knowledge and abilities to potential employers from the public and private sectors. Full details are available at http://forensecure.sat.iit.edu/.

Students in our graduate curricula have been called upon to conduct research in public cloud forensics for the FBI and present their findings at the Chicago Regional Computer Forensics Laboratory.

Industry Professor of Information Technology and Management William Lidinsky has conducted courses in digital forensics and evidence for the Cook County Public Defender’s Office, allowing these attorneys the opportunity to better represent their clients in cases involving cybertechnology.

As part of our NxtGen Tech Program, a summer outreach program for high school students and K-12 teachers, we have one course solely on IA topics, “Computer Hacking Prevention”, and another with a significant IA component, “Building and Securing a Network: Hands-On System Administration”. These courses are offered at our Main Campus in Chicago and our Rice Campus in Wheaton. For full information, please see the flyer at https://appliedtech.iit.edu/sites/sat/files/elements/ITM/NxtGen%20Techcamp/NxtGen_Tech_Program_flyer_2015_final.pdf
2. **Center for IA/CD Education.** The institution must have a formal organization for use as a resource for faculty and students. The Center should provide program guidance, general IA/CD information and promote collaboration and interaction with other students, faculty, and programs. **The Center and the website must be operational, dynamic and current.**

**Overall Point Value: 14 points minimum/20 points maximum**

a. Show formal documentation of the designation of the IA/CD/Cybersecurity “Center” and provide a hyperlink to the “Center.”

**Point Value: 5 points required**

The IIT Center for Cyber Security and Forensics Education (C²SAFE) was established by the IIT School of Applied Technology in December 2012. Details of the Center can be found at http://c²safe.iit.edu. The establishment letter and the Charter of the Center can be viewed at http://appliedtech.iit.edu/sites/saf/files/elements/ITM/pdfs/CCSAFE_Establishment_Letter_final.pdf

b. Demonstrate the “Center” website is operational, dynamic and current: contains up-to-date links to key IA/CD resources such as other academic institutions, government sites, conferences, workshops, IA/CD news, center POCs, IA/CD courses, etc. The website must be easy to find and easily accessible. Demonstrate how students know about the website.

**Point Value: 5 points required**

IIT Center for Cyber Security and Forensics Education (C²SAFE) website is active and operational at http://c²safe.iit.edu. Students can find the website from pages in the IIT School of Applied Technology website: http://appliedtech.iit.edu/information-technology-and-management/about/innovation/cyber-system-and-network-security-and http://appliedtech.iit.edu/information-technology-and-management/current-students. Students can also Google “C²SAFE” or “ForenSecure”.

c. Provide evidence that subscription-based, on-line IA/CD journals are available for student and faculty use. Demonstrate that hyperlinks to key IA/CD on-line resources are provided in course syllabus and/or professors’ webpage or provided to students during class instruction.

**Point Value: Up to 5 points/2 required**

IIT’s Galvin Library has extensive journal holdings in IA. The full list is at http://appliedtech.iit.edu/sites/sat/files/elements/ITM/pdfs/IIT_Galvin_Library_Cyber_Security_Journals.pdf and the library’s full journal holdings can be searched or browsed at http://library.iit.edu/journals/.

Links to online resources within courses are typically included in IIT's Learning Management System, Blackboard, which is not publicly viewable. This makes it difficult to demonstrate apart from the links page maintained by C²SAFE at http://appliedtech.iit.edu/c²safe/resources. An example Blackboard course link page can be viewed at http://dickens.rice.iit.edu/CAEIA/Tools–ITMS-478_ITMS-578_IT-S-478-Parent.pdf

d. Demonstrate that physical and/or virtual IA/CD labs and equipment are available and used for hands-on learning. (provide examples of student lab projects/exercises/case studies – syllabus, links to assignments, etc.).

**Point Value: Up to 5 points/2 required**

The IIT C²SAFE Cyber Forensics and Security Laboratory (ForSec Lab) is very active as seen by the lab’s website at http://appliedtech.iit.edu/cyber-forensics-
security. There is a main 24-seat student learning lab supported by a separate server room and an extensive project room which has its own server racks as well. The ForSec Lab is located at IIT's Daniel F. and Ada L. Rice Campus in Wheaton, Illinois. Bus transportation is provided from IIT's Main Campus in Chicago to ensure all students have the opportunity to make use of the lab facilities. A sample of a lab exercise assigned using this lab is available at http://dickens.rice.iit.edu/CAEIA/ITMS448-548_lesson03aBackOrifice-Lec&Lab.pdf

A major ongoing project of the ForSec Lab is the development of the Remotely-Accessible Dynamic Infrastructure for Students to Hack (RADISH) virtual infrastructure, which is intended to give students full, unrestricted access to ForSec Lab resources from any location and from nearly any Internet-connected device. RADISH enables 24/7 access so students may work on their projects continuously with no logistical concerns. Full details on RADISH including a technical paper are at http://appliedtech.iit.edu/cyber-forensics-security/radish. A sample laboratory exercise assigned using RADISH can be seen at http://dickens.rice.iit.edu/CAEIA/ITMS443-543Assignment4.pdf.

In addition, the IIT School of Applied Technology maintains four multiple-purpose computer labs at our campuses in both Wheaton and Chicago, normally with 24 student seats. The School also manages an additional lab for the IIT Chemical Engineering Department, which is also available for security courses conducted by the Department of Information Technology and Management. Computers supplied in the laboratories are, in most cases, configured with two removable hard drive bays, allowing the lab to be entirely reconfigured in moments for use in a variety of configurations. One hard drive set is configurable for use exclusively by our Operating System Security class which gives students complete control over their lab environment. Current systems installed or planned for these labs are configured with Quad Core Intel i7 processors, 32 GB of RAM memory, and at least two, and in many cases four, wired Ethernet ports.

The School of Applied Technology also operates an extensive virtual server infrastructure and provides both Windows and Linux servers to support teaching and learning on an as-needed basis, with VPN access for faculty and students. This infrastructure is served by two extensive storage area networks, one at each campus in Wheaton and Chicago.

The School of Applied Technology operates the IIT Real-Time Communications Laboratory with facilities in both Wheaton and Chicago. This lab conducts extensive research in networking and real-time communications, with some projects focusing on security. A recent project created an appliance that prevents steganographic theft in the RTP stream created by a VoIP call. Details of this lab can be found at http://voip.itm.iit.edu/overview.php
3. **A robust and active IA/CD academic program.** Demonstrate how students successfully participate in the academic program requirements to meet the IA/CD curriculum.

**Overall Point Value: 5 points minimum/ 20 points maximum**

a. Provide evidence that students who participate sufficiently in the IA/CD curriculum (i.e., take and pass courses that satisfy all of the mandatory KU requirements and at least five of the optional KU requirements) will receive a certificate, or a reference to completing the CAE IA/CD course of study on their transcript and/or degree. Provide evidence in the form of a letter, transcript notation, and/or degree (student information may be redacted)

**Point Value: 10 points/Students are taking the IA/CD curriculum path or**

5 points/Students have an opportunity to take the IA/CD path

Students enrolled in the co-terminal degree program encompassing the Bachelor of Information Technology and the Master of Information Technology and Management with a specialization in Computer and Information Security, or are enrolled in the co-terminal degree program encompassing the Bachelor of Information Technology and the Master of Cyber Forensics and Security, will have completed the IA/CD curriculum. Assuming that graduate students have met the prerequisites that cover the non-security-specific knowledge units, upon completion of the Master of Information Technology and Management with a specialization in Computer and Information Security, or the Master of Cyber Forensics and Security, students will have completed the IA/CD curriculum. Students completing these curriculum tracks will receive a certificate from the IIT School of Applied Technology indicating that they have completed the National Center of Academic Excellence in Information Assurance/Cyber Defense Curriculum in Information Assurance/Cyber Defence as prescribed by the United States National Security Agency and the United States Department of Homeland Security. A sample of the certificate is available for review at http://dickens.rice.iit.edu/CAEIA/InformationAssurance-CyberDefenseCertificate.pdf.


There is no method to determine students enrolled in the Master of Information Technology and Management with a specialization in Computer and Information Security as completion of specializations cannot be determined until the final semester of study.
b. Provide evidence that students who participate sufficiently in the IA/CD curriculum for a Focus Area (i.e., take and pass courses that satisfy all of the mandatory KU requirements for that Focus Area) will receive certificate, or a reference to a focus area on their transcript and/or degree (student information may be redacted).

**Point Value:**

- **10 points**/Students are taking the IA/CD curriculum path or
- **5 points**/Students have an opportunity to take the IA/CD path

We are not submitting focus areas at this time but would like to be able to do so at a later date. We do have a certificate already prepared to present to students completing a focus area, a sample of which can be reviewed at [http://dickens.rice.iit.edu/CAEIA/InformationAssurance-CyberDefenseFocusAreaCertificate.pdf](http://dickens.rice.iit.edu/CAEIA/InformationAssurance-CyberDefenseFocusAreaCertificate.pdf)
4. **IA/CD is multidisciplinary within the institution.** The institution must demonstrate that IA/CD is not treated as a separate discipline, but as a multidisciplinary science with the body of IA/CD knowledge incorporated into various disciplines.  

**Overall Point Value: 7 points minimum/ 10 points maximum**

a. Evidence that IA/CD is taught as modules in existing non-IA/CD courses and that non-technical/non-IA/CD students are being introduced to IA/CD. For example: IA topics such as security countermeasures are covered in courses for managers/leaders/non-technical students.

**Points: 1 point per course/2 courses required/up to 5 points**

- **ITM 100, Introduction to Information Technology as a Profession** is required for incoming freshmen to introduce them to the faculty and their chosen profession. This course “leads students to recognize the need for continuing professional development, and imparts an understanding of professional, ethical, legal, security and social issues and responsibilities information technology.” (emphasis added) Weeks 14 and 15 of the course address Information Security. Syllabus: [Link](http://dickens.rice.iit.edu/CAEIA/ITM100Syllabus15S.pdf)

- **ITMO 454/554, Operating System Virtualization** covers technologies allowing multiple instances of operating systems to be run on a single physical system. According to the course description, “Business benefits, business cases, and security implications of virtualization will be discussed.” (emphasis added) Week 14 of the course addresses Security Implications of Virtualization. Syllabus: [Link](http://dickens.rice.iit.edu/CAEIA/ITMO454-554_Syllabus_Spring15_McHugh.pdf)

- **ITMM 485/585, Legal and Ethical Issues in Information Technology**, covers current legal issues in information technology as well as current and future ethical issues to equip students to make sound ethical choices and resolve legal and moral issues that arise in information technology. Week 5 of the course addresses Privacy, week 6 covers Security and Compliance, and week 7 covers CyberCrime and Technology-Facilitated Crime. Syllabus: [Link](http://dickens.rice.iit.edu/CAEIA/ITMM485-585syllabus15S.pdf)

- **ITMO 556, Introduction to Open Source Software** is taken by graduate students to introduce them to concepts, mechanisms and execution of Open Source Software, and to introduce them to the Linux operating system. Security is addressed in the Course Description and is covered in week 16 of the course. Syllabus: [Link](http://dickens.rice.iit.edu/CAEIA/ITMO556syllabus15S.pdf)

- **PA 516, Information Technology and Public Administration** is a course taught to non-technical students in the Master of Public Administration curricula by IIT's Stuart School of Business. The course helps “students become aware of the general management challenges that the use of information technology presents for governments and to be able to develop appropriate policies that address these challenges.” Objective 6 of the course reads, “Develop an understanding of the requirements of security and privacy in the planning, design, implementation, and maintenance of government Information Technology Systems;” week 3 of the course covers Information Technology and Privacy while week 4 addresses Information Security Policy. Syllabus: [Link](http://dickens.rice.iit.edu/CAEIA/PA516_Syllabus_Summer2014_v01_from_William_Slater_.pdf)
PA 538, Information Systems Security & Cyber Crime is a course taught to non-technical students in the Master of Public Administration curricula by IIT’s Stuart School of Business. The course “provides an introduction to information systems security, an in-depth review of topics in cyber-crime issues in the public safety field and identifies methods of preventing cyber-crime in organizations. It includes issues involved with policy and legal issues of enforcement of cyber-crime laws, as well as tools used for network security”. IA topics form half of the course content and the course is entirely aimed at non-technical management. Syllabus: http://dickens.rice.iit.edu/CAEIA/PA538Syllabus.pdf

LAW 478, Computer and Network Privacy and Security: Ethical, Legal, and Technical Considerations is a course for Juris Doctor students in IIT’s Chicago-Kent College of Law. “More and more, both practice and the job market require lawyers who understand the interface between law and technology. This course provides a unique opportunity to understand that interface. No technical knowledge is required. Everything is explained in plain English. The course addresses the issue of privacy in an age of surveillance. How much privacy should we demand? Why does privacy matter? How is privacy to be defined? The course addresses security issues because in the Internet age there is no privacy without security and security failures may yet lead to the end of the Internet age. The course provides a unique opportunity to really understand the interface between law and technology.” Course details are at: http://www.kentlaw.iit.edu/courses/jd-courses/jd-elective-courses/computer-and-network-privacy-and-security

LAW 495: Electronic Discovery is a course for Juris Doctor students in IIT’s Chicago-Kent College of Law. “This course teaches students the law, theory, and practice of discovery of electronically stored documents and information. The course covers the federal law governing the production of electronic documents, privilege, motions to compel, and protective orders—as well as the applicable professional standards. Students will be provided a theoretical understanding of the dominant computer algorithmic techniques used in e-discovery (search terms and predictive coding) as well as the legal, ethical, and technological problems each presents. Emphasis will be on hands-on work with e-discovery software.” As this course addresses legal, ethical, and technological problems in E-Discovery, it cannot be taught without reference to applicable compliance and cyber security requirements. Course details are at: http://www.kentlaw.iit.edu/courses/jd-courses/jd-elective-courses/electronic-discovery-prof-katz

b. Non-IA courses encourage papers in IA topics or projects. Provide links to 5 to 10 best thesis, dissertation, or projects in IA within 3 years of application. Link to actual papers required — not a subscription service. 

Points: 1 point per paper/only 2 papers per course/up to 5 points

ITM 100, Introduction to Information Technology as a Profession: “Careers in IT: Penetration Tester”
http://dickens.rice.iit.edu/CAEIA/Assignment1JobOpportunities_TendianITM100.pdf

ITM 454, Operating System Virtualization: “Forensic Analysis in Virtualization”
http://dickens.rice.iit.edu/CAEIA/Undergraduate_Assignment_1_1_esetork_SetorkErfanITM454Assignment1_1.pdf
ITM 554, Operating System Virtualization: “Virtualization Security”

ITMM 585, Legal and Ethical Issues in Information Technology: “The Enemy Within: Why Unfair Sentencing of Hackers Leaves Us Vulnerable”

PA 538, Information Systems Security & Cyber Crime: “Can a Private Virtual Network (PVN) meet the needs of the Chicago Police Department?”
5. **Practice of IA encouraged throughout the Institution.** The academic program must demonstrate how it encourages the practice of IA, not merely that it teaches IA.

*Overall Point Value: 16 points minimum/20 points maximum*

a. Provide a [link](http://www.iit.edu/ots/our_policies.shtml) to the Institution IA security plan. *(required)*

**Points: 5 points required**

http://www.iit.edu/ots/our_policies.shtml; a key document in this set is the *Use of Computer Resources Policy* at http://ots.iit.edu/policies/use-computer-resources-policy. Additional policies for university administrative computing systems can be seen at http://web.iit.edu/sites/web/files/departments/general-counsel/policies/procedure_i2_information_security_program.pdf

b. Provide name, position and job description for person or persons responsible for information security at the institution.

**Points: 5 points required**

**Ophir Trigalo, Vice Provost and Chief Information Officer**


**Position Description: Chief Information Officer**

**GENERAL DESCRIPTION:** Lead the development of strategy, implementation and operations for the technology infrastructure of IIT’s IT environment:

- Creating a vision and strategic roadmap for information technology infrastructure at the University
- Creating university-wide technical policies and standards.
- Developing, marketing and supporting additional centralized infrastructure services.
- Building a strong customer service orientation with the new IT organization.

The CIO will advance the enhancement and expansion of IIT’s core technology infrastructure and to accelerate the work of other University Information Technology units as well as the IT departments within IIT’s academic divisions and its other campus locations.

Partnering with the leaders of these decentralized IT organizations, the Chief Technology Officer leads the definition of overall technology architecture standards and services for the University in the context of a comprehensive strategic plan for information technology, systems and services at IIT.

**Key Responsibilities:** Provides strategic and tactical planning, development, evaluation, and coordination of the information and technology systems for IIT. In addition, provide leadership and planning for the development of technology to support instructional needs, including media, libraries and distance education.

- Oversees the management of multiple information and communications systems and projects, including voice, data, imaging, office automation, computer operations and the Banner information system.
- Oversees the design, implementation and evaluation of the systems that support end users in the productive use of computer hardware and software.
- Oversees the development and implementation of user-training programs, especially for Banner processes.
- Provides leadership to enhance access to and security for all networked resources and information systems.

**Communications:** Facilitates communication between staff, management, vendors, and other technology resources within the organization.

**Customer Service:** Lead the development of a first-class service organization that engenders trust from the University community.
Supervision & Budget Authority: 5 director level reports

Education & Experience: Requirements: an undergraduate degree, ideally in computer science, engineering or mathematics

Experience: 15-20 years of progressive information technology experience in a collaborative customer-service focused environment.

Knowledge & Skills: Substantial knowledge and skill in leading major network, systems and data center technology organizations and projects is required along with demonstrated ability to develop an enterprise-technology architecture and to lead implementation of major technology projects. Banner implementation experience.

c. Provide evidence of the implementation of the Institution’s IA security plan that encourages IA awareness throughout the campus. (e.g., Students, faculty and staff are required to take computer based training or on-line tutorials; a security banner statement is present on institution or department computers; security related help screens are available; students are provided with a guide on good security practices, etc. - 2pts awarded per item).

Points: 6 points required/10 points maximum

Units of the university are regularly alerted to relevant security concerns through IIT Today (university news) and college-level blog entries. Examples of these follow below:

Chicago-Kent College of Law, Information Technology Services > Best Practices
http://kentlaw.iit.edu/current-students/information-technology-services/best-practices


Stuart School of Business > Don’t Be a Victim! Learn How to Identify Phishing Messages http://stuart.iit.edu/news/2013/nov/25/don%E2%80%99t-be-victim-learn-how-identify-phishing-messages


Office of Technology Services Policy Awareness

1) OTS is a presenter at the new student orientations, during which OTS staff discuss IIT’s computer policies. There is time available for questions, should any of the students wish to know more about these policies. IIT’s computer policies are also referenced, together with a link, in the University Student Handbook at https://web.iit.edu/student-affairs/handbook/fine-print/policies-regulations-and-procedures. The IIT Code of Conduct explains that violations of computer policies are subject to discipline at https://web.iit.edu/student-affairs/handbook/fine-print/code-conduct

2) CIO Ophir Trigalo is a presenter at the new faculty orientation during which he mentions IIT’s Use of Computer Resources Policy and the policies and procedures for addition or removal of lab software.
3) Before anyone at IIT can access IIT's network, he/she must agree to IIT's Use of Computer Resources Policy through a dialog presented as part of the Network Registration process.

4) Starting this fall, OTS will be providing User Guides targeted to students, faculty and staff that will point each group in the direction of IIT's computer policies.

Evidence of the Office of Technology Services Policy Awareness efforts cited above are in an email from OTS; this document is available at http://dickens.rice.iit.edu/CAEIA/OTSPoliciesEmail.pdf
6. **Student-based IA/CD/Cybersecurity research.** The institution must demonstrate how it encourages research in IA/CD. This criterion focuses on **STUDENT-based** research and is important because research fuels the relevancy and currency of IA curricula. Research should relate back to one or more KUs.

**Overall Point Value: 10 points minimum/30 points maximum**

a. Program with IA/CD focus has thesis, dissertation, student papers, or independent research project requirements. Focus areas include declared majors, declared minors, established certificates of study within a major that produce research papers/projects. Provide links to 5 to 10 best actual thesis, dissertation, student papers, or projects in IA within 3 years of application.

**Point Value: 1 point per paper or project/5 points required/10 points maximum**

Links to published student research in IA/CD are provided at http://appliedtech.iit.edu/sites/sat/files/elements/ITM/pdfs/Published_Student_Research_in_Cyber_Security_and_Digital_Forensics.pdf. Each item listed includes a link to the paper.

b. List IA/CD courses that require research paper(s) or virtual/physical lab project(s) within 3 years of application. Provide link to course syllabus.

**Point Value: 1 point per course/3 points required/20 points maximum**

- ITMS 484/584 - Governance, Risk, and Compliance: research paper or project [http://dickens.rice.iit.edu/CAEIA/ITMS484-584.pdf](http://dickens.rice.iit.edu/CAEIA/ITMS484-584.pdf)
- ITMS 518 - Coding Security: research paper or project [http://dickens.rice.iit.edu/CAEIA/ITMS518.pdf](http://dickens.rice.iit.edu/CAEIA/ITMS518.pdf)
- ITMS 579 - Topics in Cyber Security: varies by term but normally has a paper [http://dickens.rice.iit.edu/CAEIA/ITMS579.pdf](http://dickens.rice.iit.edu/CAEIA/ITMS579.pdf)
7. **Number of IA/CD/Cybersecurity faculty and course load.** The institution must demonstrate that IA/CD faculty consists of a sufficient number of full time IA/CD faculty members and additional faculty members (may be part-time, adjunct, visiting professor, etc.) teaching at least one IA/CD course. This criterion requires a link to a **biography** or **curriculum vitae** for each faculty member.  
**Overall Point Value: 8 points minimum/16 points maximum**

   a. Identify by name full-time employee or employees, as defined above, either faculty or member of the administration working in IA with overall responsibility for the IA Instructional Program. Provide evidence, i.e., letter of testimony or job description. **Provide link to biography or CV.**  
   **Point Value: 5 points required**
   Industry Professor of Information Technology & Management Raymond Trygstad is the Interim Associate Director of the IIT Center for Cyber Security and Forensics Education. Additionally Professor Trygstad is the Associate Chair of the Department of Information Technology & Management and Chair of the Department’s Curriculum committee, and as such is the curriculum manager for the department. Evidence is in the establishment letter of the Center at [http://appliedtech.iit.edu/sites/sat/files/elements/ITM/pdfs/CCSAFE_Establishment_Letter_final.pdf](http://appliedtech.iit.edu/sites/sat/files/elements/ITM/pdfs/CCSAFE_Establishment_Letter_final.pdf) and the ITM Curriculum Committee Appointment Letter at [http://dickens.rice.iit.edu/CAEIA/2013CurriculumCommitteeFacultyAppointment.pdf](http://dickens.rice.iit.edu/CAEIA/2013CurriculumCommitteeFacultyAppointment.pdf)
   Biographies for both professors are at [http://appliedtech.iit.edu/sites/sat/files/elements/ITM/pdfs/Members_of_the_Center_for_Cyber_Security_and_Forensics_Education.pdf](http://appliedtech.iit.edu/sites/sat/files/elements/ITM/pdfs/Members_of_the_Center_for_Cyber_Security_and_Forensics_Education.pdf)

   b. Identify by name additional full-time IA faculty members (not listed in 7.a.), teaching IA/CD courses within the department that sponsors IA/CD programs. **Provide link to biography or CV.** **Point Value: 2 point each/6 points maximum**
   At this time there are no additional full time faculty teaching IA/CD courses within the department.

   c. Identify by name part-time, shared (inter departmental, other institution, etc.), adjunct (industry expert, etc.) teaching IA/CD courses within the department that sponsors IA/CD programs. **Provide link to biography or CV.** **Point Value: 1 point each/5 points maximum**
   Adjunct Industry Professor of ITM Bonnie A. Goins
   Adjunct Instructor of ITM Shawn Davis
   Adjunct Instructor of ITM Sean Hughes-Durkin
   Adjunct Industry Professor of ITM William Slater
   Adjunct Industry Associate Professor of ITM Kevin Vaccaro
   (Professor Vaccaro is shared faculty with Moraine Valley College)
   Biographies for both all faculty members listed above are at [http://appliedtech.iit.edu/sites/sat/files/elements/ITM/pdfs/Members_of_the_Center_for_Cyber_Security_and_Forensics_Education.pdf](http://appliedtech.iit.edu/sites/sat/files/elements/ITM/pdfs/Members_of_the_Center_for_Cyber_Security_and_Forensics_Education.pdf)
8. **Faculty active in current IA/CD/Cybersecurity practice and research.** The institution must clearly demonstrate that the faculty is active in current IA/Cyber practice and research, contributes to IA literature, and are members of IA professional societies are subject matter experts or attend/present at professional IA conferences.

**Overall Point Value: 15 points minimum/37 points maximum**

a. Peer reviewed publications – papers (electronic or traditional) on IA/CD/Cybersecurity as evidenced in refereed journals or conference proceedings within the past 3 years. **Provide links to actual papers not subscription service.**

**Point Value: 2 points per paper/8 points maximum**

The listing of faculty research with links to papers is at [http://appliedtech.iit.edu/sites/sat/files/elements/ITM/pdfs/Recent_IIT_Faculty_Research_in_Cyber_Security_and_Digital_Forensics.pdf](http://appliedtech.iit.edu/sites/sat/files/elements/ITM/pdfs/Recent_IIT_Faculty_Research_in_Cyber_Security_and_Digital_Forensics.pdf)

b. Published books or chapters of books on IA/CD/Cybersecurity. Books/chapters must focus on IA and have been published within the last 5 years. **Provide title, authors and date published. ID specific chapters if authoring a chapter of a book.**

**Point Value: 5 points per book/1 point per chapter/10 points maximum**

“Chapter 11. CERT Resilience Management Model: An Overview”

**Author:** Bonnie A. Goins Pilewski, Department of Information Technology and Management, Illinois Institute of Technology

Christopher Pilewski, Aurora, Illinois

**Published in:** *Information Security Management Handbook, Sixth Edition, Volume 6*

Harold F. Tipton and Micki Krause Nozaki, Editors

Auerbach Publications ©2012

Pages 135–152


DOI: 10.1201/b11802-17


c. Faculty is involved in writing grants and obtaining funding for IA education and/or research development or lab equipment. Provide synopsis of IA related grants, funding, equipment donations, or other funding to include date and approximate monetary value for the past 3 years.

**Point Value: 2 points per award/6 points maximum**

There are no active grants in the Department of Information Technology and Management.

d. Faculty members are subject matter experts (IA/CD/Cybersecurity) for accrediting bodies and professional societies for IA/CD/Cybersecurity, (e.g., ACM, IEEE, regional accreditation, professional accreditation, etc.). Faculty members are active members in IA/CD/Cybersecurity organizations (e.g., ISSA, Cyberwatch, InfraGuard, etc.) **List involvement for the last 3 years. Point Value: 2 points per review/membership/6 points maximum**

Professors Trygstad, Goins, and Slater are members of the Information Systems Audit and Control Association (ISACA).

Professor Trygstad is an ABET Program Evaluator for Information Technology programs and is an ISACA Academic Advocate.

Professor Goins is a member of the International Information Systems Security Certification Consortium (ISC)².
Professor Slater is member of the EC Council and the Federal IT Security Institute (FITSI).

e. Faculty members are engaged in and/or initiate student IA programs. **Point Value: 1 points per program/3 points maximum**
   We do not know what this means.

f. Faculty presents IA/CD/Cybersecurity content at major Regional/National/International conferences and events. Provide synopsis of involvement for the last 3 years. **Point Value: 1 point per conference/4 points maximum**
   Faculty members have presented at ForenSecure, IIT’s regional conference and expo on cyber security and digital forensics for every year of the eleven years the conference has been held.
   
   Presenters at ForenSecure ’14 included Professors Goins and Slater. (http://forensecure.sat.iit.edu/2014/content/session-abstracts)

   Presenters at ForenSecure ’13 included Professors Trygstad, Goins, and Slater, ITM Instructor Shawn Davis, and IIT Professor of Law Richard Warner. (http://forensecure.sat.iit.edu/2013/content/session-abstracts)

   ForenSecure ’12 featured a presentation by Professor Trygstad, who was also a member of a panel discussion on Public Policy and the Internet. (http://www.cvent.com/events/forensecure-12-it-forensics-and-security-conference-and-expo/custom-18-3496b59fea7748d3ad66d7118c1b6db8.aspx)