Prerequisites
None. CSP: 1, 2, 3, 4, 5, 6, 7, 8.

Required Materials

Course readings consist of published research journal articles, published cases, and certain online reports and publications. These are generally available via study.net or downloadable directly from the source without charge. No textbook is required.

See “Readings” below for a complete list of required reading material.

Catalog Description
This course is designed to develop knowledge and skills for the management and assurance of security of information and information systems in technology-enabled environments. It focuses on concepts and methods associated with planning, designing, implementing, managing, and
auditing security at all levels on different platforms, including worldwide networks for e-

business. The course presents techniques for assessing risk associated with accidental and
intentional breaches of security and covers the associated issues of ethical uses of information
and privacy considerations.

**Course Objectives**

Students completing this course will be capable of:

1. distinguishing the relationships of various information systems elements with threats and
   security features that protect the elements from these threats, viz.,
   a. applying a TFO Model to an organizational setting,
   b. using a comprehensive IT Threats Framework to develop scenarios for an
      organizational setting,
   c. using an IT Safeguards Framework to develop alternatives for IT security
      controls,
2. analyzing and evaluating the ethics of information development and use, viz.,
   a. incorporating Privacy Law into security planning,
   b. incorporating public accounting legal requirements (e.g., SARBOX) into security
      planning,
3. planning, designing, and implementing IT security, viz.,
   a. organizing and planning IT Risk Management operations,
   b. organizing the IT security function,
   c. adapting an organizational IT security methodology,
   d. constructing organizational policies,
4. auditing IT security, viz.,
   a. applying security standards (e.g., COBIT) to an organizational setting,
   b. determining organizational compliance with security standards, privacy laws, and
      public disclosure laws.

**Special Considerations**

The course web site will be used as a repository for further required course material that arises
during the class. The main online tool for team projects is Desire2Learn. Students must arrange
for their own access to the World Wide Web (Internet access is available free in the GSU labs)
and must establish their access capability to Desire2Learn. All student work submitted in
fulfillment of course requirements is deemed to be granted in the public domain (copyright-free)
for the purposes of use as instructional material or examples of student work in future courses.
Constructive assessment of this course by students plays an indispensable role in shaping
education at Georgia State. Upon completing the course, students are asked to take the time to
fill out the online course evaluation. The course syllabus provides a general plan for the course.
Deviations may be necessary.

**Method of Instruction**

Classroom sessions will regard the same topics as the readings assignments, but seek further
depth through discovery learning. It is essential that students read the assigned material before
coming to class. Instruction will follow these three approaches: (1) topic discussion of course
principles and concepts, (2) discussion of cases that will apply knowledge of information
security concepts to actual business settings, and (3) class activities that apply these concepts to simulated business situations. Preparation is essential and all students are required to have read, and be prepared to discuss critically, the readings assigned. Individuals may be “cold called” to introduce an article or to initiate discussion. In assigning the participation grade, both class attendance and the quality of oral contributions during class discussions will be considered.

**Class Attendance Policy**

Students are not permitted to miss classes without prior arrangements. In cases of absence due to emergency, contact the instructor as soon as possible. It is the student’s responsibility to attend class, obtain assignments, and turn in work on time. Absence from class does not relieve students of these responsibilities. Unless an absence is excused, students will NOT be allowed to make up missed work.

**Flicker and Noise Distractions**

By continued enrollment in this class, students agree to practice a “click-free”, “flicker-free” and “noise-free” environment for fellow students in this classroom. Students agree that mobile devices will be silenced and unused except for in-class purposes. Students agree to forebear from the use of computers during the class for email, web-surfing, gaming, social-networking etc.

**Withdrawals**

Students who withdraw before the midpoint will receive a grade of W. Students withdrawing after this date will receive a grade of WF unless a hardship authorization is obtained from the Dean of Students. For the exact midpoint date see http://calendar.gsu.edu/calendar.

**Incompletes**

A grade of I will be given only in exceptional circumstances. A student must have completed all but one of the requirements of the course in order to be eligible to receive a grade of I.

**Assessment**

Learning objectives will be assessed by both individual and group performance through the following course features:

**Discussions**

The course will include in-class discussions of assigned readings and six cases: (1) Secom, (2) TJX, (3) ChoicePoint, (4) Leih’s ITPM Case, (5) Google, and (6) Sony. Students will have individual opportunities to contribute thoughtful and critical oral observations during class discussions focused on the course objectives. There will be readings assigned for most class meetings. Students will have opportunities during the semester to introduce and comment on these readings during in-class discussions. An email group server provides opportunities for discussions outside of class meeting times.

**Team Activities**

Four in-class team activities will be organized: (1) Threat scenarios, (2) Threat news reports, (3) Methodology bends, (4) Ethical hacking demonstration. Assessment of performance is generally based on the quality of the deliverables in each activity and student evaluations of deliverables
may be components of this assessment. These activities will be competitive and are further
detailed in the activity descriptions distributed before the activities.

Students will form self-managing teams for the purpose of completing team activities. Each
team is expected to persist through the course. Peer appraisals may be part of the overall
grading/evaluation of individual performance. Consensus on the relative contributions of each of
the team members will be derived through assessment of documented facts and records,
evaluation of team output, and evaluation of team processes. Unless team members inform the
instructor in writing to the contrary, the assumption will be that each team member contributed
equally to the assessed products of the team.

**Quizzes**
There will be two short, objective, multiple-choice quizzes that assess familiarity with the
principles and general organization of two examples of security management frameworks: (1)
CobiT, and (2) Octave.

**Tradeshow Participation**
Each team will prepare a class tradeshow entry that critically explains and assesses an approved
commercially available information security product. The entry must demonstrate the students’
ability to research a technical problem and its solutions, analyze data, synthesize data from
different sources, and to compare and to evaluate distinct solution products with a clear train of
fact-based argumentation. Any and all conclusions and recommendations must be clearly stated.
To insure research originality, students are strongly encouraged to seek information beyond web
pages, and from at least one original source (such as an interview with an authority on the
subject). The entry must be authoritative, including citations and full references to all direct
sources. Student team evaluations of tradeshow entries are components of this assessment.

### Grading Policy

<table>
<thead>
<tr>
<th>Activity</th>
<th>Points Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case and readings discussions</td>
<td>400</td>
</tr>
<tr>
<td>Team activities</td>
<td>300</td>
</tr>
<tr>
<td>Quizzes</td>
<td>100</td>
</tr>
<tr>
<td>Tradeshow</td>
<td>200</td>
</tr>
<tr>
<td>Total</td>
<td>1000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Letter Grade</th>
<th>Percentage Range</th>
<th>Point Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>A+</td>
<td>&gt;96% - 100%</td>
<td>&gt;960 - 1000</td>
</tr>
<tr>
<td>A</td>
<td>96% - 98%</td>
<td>900 - 959</td>
</tr>
<tr>
<td>A-</td>
<td>92% - 95%</td>
<td>870 - 900</td>
</tr>
<tr>
<td>B+</td>
<td>88% - 90%</td>
<td>830 - 880</td>
</tr>
<tr>
<td>B</td>
<td>82% - 85%</td>
<td>800 - 830</td>
</tr>
<tr>
<td>B-</td>
<td>79% - 82%</td>
<td>770 - 800</td>
</tr>
<tr>
<td>Letter Grade</td>
<td>Percentage Range</td>
<td>Point Range</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>C+</td>
<td>73% - 76%</td>
<td>730 - 769</td>
</tr>
<tr>
<td>C</td>
<td>70% - 72%</td>
<td>700 - 729</td>
</tr>
<tr>
<td>C-</td>
<td>67% - 69%</td>
<td>670 - 699</td>
</tr>
<tr>
<td>D</td>
<td>60% - 66%</td>
<td>600 - 669</td>
</tr>
<tr>
<td>F</td>
<td>0% - 59%</td>
<td>0 - 599</td>
</tr>
</tbody>
</table>

**Readings**

Note: Accessing some of these resources may only be completed from an on-campus computer or through a VPN connection from off-campus. An on-campus IP address is usually required. For more information see “Connecting to the Network from Home (VPN - Virtual Private Network)” at [http://www.gsu.edu/help/25697.html](http://www.gsu.edu/help/25697.html).


---

**Academic Honesty**


As members of the academic community, students are expected to recognize and uphold standards of intellectual and academic integrity. The University assumes as a basic and minimum standard of conduct in academic matters that students be honest and that they submit for credit only the products of their own efforts. Both the ideals of scholarship and the need for fairness require that all dishonest work be rejected as a basis for academic credit. They also require that
students refrain from any and all forms of dishonorable or unethical conduct related to their academic work.

Students are expected to discuss with faculty the expectations regarding course assignments and standards of conduct. Here are some examples and definitions that clarify the standards by which academic honesty and academically honorable conduct are judged at GSU.

**Plagiarism.** Plagiarism is presenting another person’s work as one’s own. Plagiarism includes any paraphrasing or summarizing of the works of another person without acknowledgment, including the submitting of another student’s work as one’s own. Plagiarism frequently involves a failure to acknowledge in the text, notes, or footnotes the quotation of the paragraphs, sentences, or even a few phrases written or spoken by someone else. The submission of research or completed papers or projects by someone else is plagiarism, as is the unacknowledged use of research sources gathered by someone else when that use is specifically forbidden by the faculty member. Failure to indicate the extent and nature of one’s reliance on other sources is also a form of plagiarism. Failure to indicate the extent and nature of one’s reliance on other sources is also a form of plagiarism. Any work, in whole or part, taken from the Internet or other computer based resource without properly referencing the source (for example, the URL) is considered plagiarism. A complete reference is required in order that all parties may locate and view the original source. Finally, there may be forms of plagiarism that are unique to an individual discipline or course, examples of which should be provided in advance by the faculty member. The student is responsible for understanding the legitimate use of sources, the appropriate ways of acknowledging academic, scholarly or creative indebtedness, and the consequences of violating this responsibility.

**Cheating on Examinations.** Plagiarism is presenting another person’s work as one’s own. Plagiarism includes any paraphrasing or summarizing of the works of another person without acknowledgment, including the submitting of another student’s work as one’s own. Plagiarism frequently involves a failure to acknowledge in the text, notes, or footnotes the quotation of the paragraphs, sentences, or even a few phrases written or spoken by someone else. The submission of research or completed papers or projects by someone else is plagiarism, as is the unacknowledged use of research sources gathered by someone else when that use is specifically forbidden by the faculty member. Failure to indicate the extent and nature of one’s reliance on other sources is also a form of plagiarism. Failure to indicate the extent and nature of one’s reliance on other sources is also a form of plagiarism. Any work, in whole or part, taken from the Internet or other computer based resource without properly referencing the source (for example, the URL) is considered plagiarism. A complete reference is required in order that all parties may locate and view the original source. Finally, there may be forms of plagiarism that are unique to an individual discipline or course, examples of which should be provided in advance by the faculty member. The student is responsible for understanding the legitimate use of sources, the appropriate ways of acknowledging academic, scholarly or creative indebtedness, and the consequences of violating this responsibility.

**Unauthorized Collaboration.** Submission for academic credit of a work product, or a part thereof, represented as its being one’s own effort, which has been developed in substantial collaboration with assistance from another person or source, or computer honesty. It is also a violation of academic honesty knowingly to provide such assistance. Collaborative work specifically authorized by a faculty member is allowed.
# Course Schedule (Subject to Change)

<table>
<thead>
<tr>
<th>Week</th>
<th>Part</th>
<th>Lesson Topic</th>
<th>Deliverables</th>
<th>Preparation Reading</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>Syllabus &amp; Plan</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Visitor: Joel Glogowski – Biz Librarian</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Principles Discussion: TFO &amp; Incident centered security management</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Aperitif: Privacy and Security in the Cloud</td>
<td>Optional Reading: (Whitley et al., 2013)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>Team Activities: Team News Organization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>Principles Discussion: Organizational context of IT Security (COBIT)</td>
<td>IT Resources: (IT Governance Institute, 2007, read pp. 5-28)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Case Discussion: Management of IS Security</td>
<td>Secom Case: (McFarlan et al., 2008)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Principles Discussion: IT Threats</td>
<td>Risk Mgmt: (Tsohou et al., 2006)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Team Activity: Threats scenarios for Jashopper</td>
<td>Team scenarios &amp; evaluations</td>
<td>Octave Scenarios (Caralli et al., 2007, p. 48-52)</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>Principles Discussion: IT Safeguards Framework ISO 17799 / 27002</td>
<td>Security Standards: (Backhouse et al., 2006)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Case Discussion TJX</td>
<td>TJX Case (Xu et al., 2008)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Confirmed Visitors: Dan Schroeder, Daniel James, HA&amp;W</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>Principles Discussion: Privacy</td>
<td>Privacy: (Baumer et al., 2004)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Case Discussion: ChoicePoint</td>
<td></td>
<td>Choicepoint A case study (Paine &amp; Phillips, 2008)</td>
</tr>
<tr>
<td>Week</td>
<td>Date</td>
<td>Part</td>
<td>Lesson Topic</td>
<td>Deliverables</td>
</tr>
<tr>
<td>------</td>
<td>------</td>
<td>------</td>
<td>--------------</td>
<td>--------------</td>
</tr>
</tbody>
</table>
| 3    |      | 3    | Principles discussion: Control Technologies | Limits of Legal: (Samuelson, 2012)  
                                          Passwords: (Charoen et al., 2008)  
                                          (Hathaway et al., 2012, pp. 819-839) | |
|      |      | 4    | Quiz: COBIT  |              |                      |
|      |      | 5    | Après Quiz: Big Data | Police & Big Data (Joh, 2014) | |
| 5    |      | 1    | Principles discussion: Regulation by SARBOX, HIPPA, etc. | Regulation Risk: (Berghel, 2005),  
                                          SOX 404 compliance (Wallace et al., 2011) | |
|      |      | 2    | Confirmed Visitors: Charles Britt, Darren Highfill, PwC | TJX Case Audit (Berg et al., 2008) | |
|      |      | 3    | Principles discussion: IT Audit & Disclosure | | |
|      |      | 4    | Case Discussion: IT Project Management Audit Case | Leih’s I TPM Case (Leih, 2006, read pp. 20-28) | |
| 6    |      | 1    | Principles: Hacking and scams | Scams: (Stajano & Wilson, 2011)  
                                          Phishing: (Herzberg, 2009) | |
|      |      | 2    | Case Discussion  
                                          Google China (B) | Google Case: (Compeau et al., 2010) | |
|      |      | 3    | Principles discussion: IT security methodology | (Alberts & Dorofee, 2001) | |
|      |      | 4    | Team activity: Ethical hacking demonstrations | Demonstration script | |
|      |      | 2    | Confirmed Visitor: Peter Chronis, Earthlink | | |
|      |      | 3    | Quiz: Octave | | |
|      |      | 4    | Team Activity: Methodology Bends | Adaptation & Evaluation | |
| 8    |      | 1    | Principles discussion: IT Risk Management | Risk Analysis: (Rees & Allen, 2008)  
                                          Measuring Risk: (Pfleeger & Cunningham, 2010) | |
|      |      | 2    | Tradeshow | Entry Brochure | |