

Quality Enhancement Plan (QEP): From These Roots ... A Foundation for Life: Mathematics and Financial Literacy

CSC 485 Risk Management

Instructor: **Office:** S&T 120 **Telephone:**

Office Hours: (tentative: to be reset in the next couple of weeks)

E-Mail:

Course Description: Outlines the aspects of computer security and risk management. Accreditation, implementation, extension, and operation principles for secure information systems. Security policy and plan development. Contingency, continuity and disaster recovery planning. Incident handling and response. Prerequisite: CSC382 or Consent of the Chair.

Course Objectives: This course focuses on teaching and training students to be able to describe the procedure and apply the implementation of risk management in a secure manner, as well as be able to perform the comprehensive assessment and identification of risk and deploy appropriate risk control strategies. This course also covers security policy and plan development, business continuity plan, disaster recovery plan, incident handling and response. After completing the course, students would be able to

- Discuss and identify risk.
- Discuss and perform risk management.
- Discuss and perform of risk assessment.
- Discuss and implement risk control strategies.
- Discuss and develop security policy and plan.
- Discuss and implement business continuity plan.
- Discuss and implement disaster recovery plan.
- Discuss and perform the procedure of incident handling and response.

Minimum Competencies: Students meeting minimum competencies should expect to receive a grade between 74% and 77%. Minimum competencies for this course are as follows:

- Discuss and identify risk.
- Discuss and perform risk management.
- Discuss and perform of risk assessment.
- Discuss and implement risk control strategies.
- Discuss and develop security policy and plan.
- Discuss and implement business continuity plan.
- Discuss and implement disaster recovery plan.
- Discuss and perform the procedure of incident handling and response.

Course Topics: This course will cover most of the information assurance concepts including:

Quality Enhancement Plan (QEP): From These Roots ... A Foundation for Life: Mathematics and Financial Literacy

- Risk Management Overview (3 hours)
- Risk Identification (3 hours)
- Risk Assessment (6 hours)
- Risk Control Strategies (1.5 hours)
- Selecting a Risk Control Strategy (1.5 hours)
- Risk Mitigation (3 hours)
- Quantitative versus Qualitative Risk Control Practices (1.5 hours)
- Risk Management Discussion Points (1.5 hours)
- Security Policy and Plan (3 hours)
- Business Continuity Plan (3 hours)
- Disaster Recovery Plan (3 hours)
- Incident Handling and Response (3 hours)
- Laboratory (12 hours)
- *Mapping to CNSI 4012 can be found here.*

Textbooks:

- **(Whitman)** Principle of Information Security, 2nd edition, Michael E. Whitman & Herbert J. Mattord, Thomson, 2005.
- **(Krutz)** The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams, 2nd edition, Ronald L. Krutz and Russell Dean Vines, Wiley, 2004.
- **(Pfleeger)** Security in Computing, 3rd edition (or the newest), C. P. Pfleeger, S. L. Pfleeger, Prentice Hall, 2003

Supplemental Materials (SM):

- SM-1: NIST SP-30 Risk Management Guide for Information Technology Systems
- SM-2: NIST SP 800-61-rev1 Computer Security Incident Handling Guide
- SM-3: Administrative Communications System - US Department of Education
- SM-4: GAO-AIMD-12-19-6 Federal Information System Controls Audit Manual
- SM-5: IETF RFC 3227 Guidelines for Evidence Collection and Archiving
- SM-6: Army Regulation 25-2 Information Assurance
- SM-7: NIST SP 800-53-rev2-final Recommended Security Controls for Federal Information Systems
- SM-8: NISTIR 4909 Software Quality Assurance - Documentation and Reviews

Tentative Course Outline: Regular class schedule **MWF 11:00 ~ 11:50 AM**

Week	Topics	Text chapters (see 4012 map for the details)	Supplemental Materials	Tests / Programs
1	1. Risk Management Overview 1.1 Important of Risk Management (SM-1) 1.2 Life Cycle System Security Planning (SM-8) 1.3 Integration of Risk Management into System Development Life Cycle (SM-1) 1.4 Key Roles (SM-1)	Krutz: Ch1, Appendix Whitman: Ch4	SM-1, SM-8	

Quality Enhancement Plan (QEP): From These Roots ... A Foundation for Life: Mathematics and Financial Literacy

2	<ul style="list-style-type: none"> 2. Risk Identification 2.1 Asset Identification, Valuation, and Prioritization 2.2 Information Asset Classification 2.3 Information Asset Valuation 2.4 Information Asset Prioritization 2.5 Data Classification and Management 	<ul style="list-style-type: none"> Krutz: Ch1, Appendix Whitman: Ch4 Pfleeger: Ch1 	SM-1	HW-1
3	Laboratory			
4	<ul style="list-style-type: none"> 3. Risk Assessment 3.1 System Characterization (SM-1) 3.2 Threat Identification (SM-1) 3.3 Vulnerability Identification (SM-1) 3.4 Control Analysis (SM-1) 	<ul style="list-style-type: none"> Krutz: Ch1, Appendix Whitman: Ch4 	SM-1	HW-2
5	<ul style="list-style-type: none"> 3.5 Likelihood Determination (SM-1) 3.6 Impact Analysis (SM-1) 3.7 Risk Determination (SM-1) 3.8 Control Recommendations (SM-1) 3.9 Result Documentation (SM-1) 	<ul style="list-style-type: none"> Krutz Ch1, Ch6, Ch12, Appendix Whitman: Ch4 	SM-1	
6	<ul style="list-style-type: none"> 4. Risk Control Strategies 4.1 Avoidance 4.2 Transference 4.3 Mitigation (SM-1) 4.4 Acceptance 5. Selecting a Risk Control Strategy 5.1 Feasibility Studies 5.2 Cost Benefit Analysis (SM-1) 5.3 Evaluation, Assessment, and Maintenance of Risk Controls 	<ul style="list-style-type: none"> Krutz: Ch1, Appendix Whitman: Ch4 	SM-1	HW-3
7	Laboratory			
8	<ul style="list-style-type: none"> 6. Risk Mitigation 6.1 Risk Mitigation Options (SM-1) 6.2 Risk Mitigation Strategy (SM-1) 6.3 Control Categories (SM-1) 6.4 Residual Risk (SM-1) 	<ul style="list-style-type: none"> Krutz: Ch1, Appendix Whitman: Ch4 	SM-1	HW-4
9	<ul style="list-style-type: none"> 7. Quantitative versus Qualitative Risk Control Practices 7.1 Benchmarking and Best Practices 7.2 Other Feasibility Studies 8. Risk Management Discussion Points 8.1 Risk Appetite 8.2 Documenting Results 8.3 Recommended Risk Control Practices 	<ul style="list-style-type: none"> Whitman: Ch4 		
10	Laboratory			HW-5

Quality Enhancement Plan (QEP): From These Roots ... A Foundation for Life: Mathematics and Financial Literacy

11	<p>9. Security Policy and Planning</p> <p>9.1 Policy (SM-2, SM-3, SM-4, SM-5)</p> <p>9.2 The Information Security Blueprint</p> <p>9.3 Security Education, Training, and Awareness Program</p> <p>9.4 Continuity Strategies (SM-2, SM-6, SM-7)</p>	<p>Krutz: Ch1, Ch2, Ch6, Ch9, Ch11, Ch12, Ch15, Appendix</p> <p>Whitman: Ch4, Ch5, Ch10, Ch11, Ch12</p> <p>Pfleeger: Ch1, Ch3, Ch4, Ch8</p>	SM-2, SM-3, SM-4, SM-5, SM-6, SM-7	
12	<p>10. Business Continuity Plan</p> <p>10.1 Continuity Disruptive Events</p> <p>10.2 The Four Prime Elements of BCP</p> <p>10.3 Business Impact Analysis</p> <p>10.4 Testing the Business Continuity Plan (SM-2, SM-6, SM-7)</p> <p>10.5 Business Recovery (SM-2, SM-6, SM-7)</p>	<p>Krutz: Ch3, Ch5, Ch8</p> <p>Whitman: Ch5</p> <p>Pfleeger: Ch8</p>	SM-2, SM-6, SM-7	
13	Laboratory			HW-6
14	<p>11. Disaster Recovery Plan</p> <p>11.1 Goals and Objectives of DRP</p> <p>11.2 The Disaster Recovery Planning Process</p> <p>11.3 Testing the Disaster Recovery Plan</p> <p>11.4 Disaster Recovery Procedures</p> <p>11.5 Other Recovery Issues</p>	<p>Krutz: Ch 8</p> <p>Whitman: Ch5</p>	SM-2, SM-6, SM-7	
15	<p>12. Incident Handling and Response</p> <p>12.1 Organizing a Computer Security Response Capability</p> <p>12.2 Handling an Incident</p> <p>12.3 Handling Denial of Service Incidents</p> <p>12.4 Handling Malicious Code Incidents</p> <p>12.5 Handling Unauthorized Access Incidents</p> <p>12.6 Handling Inappropriate Usage Incidents</p> <p>12.7 Handling Multiple Components Incidents</p> <p>12.8 Law Enforcement Involvement (SM-2, SM-6, SM-7)</p>	<p>Krutz: Ch3</p> <p>Whitman: Ch5</p> <p>Pfleeger: Ch8</p>	SM-2, SM-6, SM-7	HW-7

Important Dates:

- Exam 1: Friday Oct. 17, 2008
- Exam 2: Friday Nov. 14, 2008
- Final Exam: Friday, Dec. 12, 2008 8:00 Am - 9:50 Am

THE FOLLOWING INFORMATION APPLIES TO ALL STUDENTS IN THE SCHOOL OF SCIENCE:

Quality Enhancement Plan (QEP): From These Roots ... A Foundation for Life: Mathematics and Financial Literacy

In addition to the minimum grade requirements established by Hampton University, all majors within the School of Science must pass all required courses offered within the School of Science with a grade of “C” or better in order to satisfy degree requirements. The minimum grade requirement is in effect for all science courses taken during Fall 2001 and beyond.

COURSE ASSIGNMENT AND CALENDAR:

Homework Assignments: There are two types of homework assignments: problems and projects. Both of them will be issued and specified with their due date in Blackboard. Problems will be used to evaluate the understanding of course materials and projects will be used to evaluate the complexity of algorithm studied in class. All of the projects must be implemented by Java in Unix/Linux environments. Late work will not be accepted and will be counted as zero.

Final Exam: The exam will be given on the date scheduled by the registrar. The exam will be comprehensive. There are no exemptions from the exam.

Attendance: The attendance policy of Hampton University will be observed. You are expected to attend all classes and to arrive on time. Your attendance and participation will be 10% of the final grade. More than **7** absences will constitute a failing grade, regardless to other considerations.

Writing-Across-The-Curriculum: Hampton University adopts the policy in all courses of “writing across the curricula”. In this course, the objectives will be achieved by homework assignments, program comments, and various tests.

The Ethics Paper: Details about the ethics paper will be provided at least one month prior to the due date. The ethics paper will be graded based on the criteria listed in “**Hampton University Scoring Rubric**”.

Grades: The final grade of this course will be determined by the combined weight of following components:

Examine (3)	20 %
Homework (7)	40 %
Laboratory (4)	15%
Attendance & participation	10 %
Ethics Paper	5 %
Final exam	10 %
-----	-----
Total	100%

Course grades will follow the scale of the university grading system:

A+	98-100
A	94-97
A-	90-93
B+	88-89

Quality Enhancement Plan (QEP): From These Roots ... A Foundation for Life: Mathematics and Financial Literacy

B	84-87
B-	80-83
C+	78-79
C	74-77
C-	70-73
D+	68-69
D	64-67
D-	60-63
F	Below 60

Make-Up Policy: No make-up tests will be given without previous arrangements, a written medical excuse, or an emergency approved by appropriate university official.

Policy on Electronic Devices: Any electronic device (i.e. cell phone, PDA, pagers, etc.) will be turned off during class. During any test or final, these devices will not be allowed at the test.

Policy on Academic Dishonesty: Please see page 29 of the Student Handbook.

Midterm Evaluation: If "F" is assigned in the midterm evaluation to a student, F will also be this student's final grade. Students should withdraw this course before the appropriate date if he/she fails the midterm evaluation.

Cheating: A student caught cheating on an examination or plagiarizing a paper which forms a part of a course grade shall be given an "F" in the course and will be subject to dismissal from the University. A student is considered to be cheating if, in the opinion of the person administering an examination (written or oral), the student gives, seeks, or receives aid during the process of the examination; the student buys, sells, steals, or otherwise possesses or transmits an examination without authorization; or, the student substitutes for another or permits substitution for himself/ herself during an examination. All cases of cheating shall be reported by the instructor to the chair of the department in which the cheating occurred, to the school dean/division director and to the Provost.

No penalty shall be imposed until the student has been informed of the charge and of the evidence upon which it is based and has been given an opportunity to present his/her defense. If the faculty member and the student cannot agree on the facts pertaining to the charge, or if the student wishes to appeal a penalty, the issue may be taken to the department chair. Each party will present his/her case to the chair who shall then call a meeting of all involved parties. If the issue is not resolved at the departmental level, the dean shall conduct a hearing. If the issue is not resolved at the school level either party may appeal the decision at the school level to the Provost who shall convene the appropriate individuals and conduct a hearing in order to resolve the issue.

Quality Enhancement Plan (QEP): From These Roots ... A Foundation for Life: Mathematics and Financial Literacy

Plagiarism: Plagiarism is defined as "taking and using as one's own the writing or ideas of another." All materials used to meet assigned written requirements of a course, from any source, must be given proper credit by citing the source. A student caught plagiarizing a paper which forms a part of a course grade shall be given an "F" in the course and will be subject to dismissal from the University.

PENALTIES FOR ACADEMIC DISHONESTY

Cases of academic dishonesty are initially investigated and reported by members of the instructional faculty to the chairperson of the department in which the cheating occurred, to the school dean, division director and to the Provost. Also, penalties for minor violations of academic dishonesty are to be recommended at the discretion of the instructor. The penalties for academic dishonesty on examinations and major course requirements may include one of the following:

1. A grade of "F" on the examination or project.
2. A grade of "F" on the examination or project and dismissal from the course.
3. A grade of "F" on the examination or project, dismissal from the course and from the University.

When dismissal from the University is the recommended penalty, the chairman of the department submits the details of the case to the Provost who schedules a hearing.

ADMINISTRATIVE ACTION

The Provost has the authority to dismiss or expel any student who fails to meet scholarship requirements or to abide by academic regulations.

Dress Code:

This code is based on the theory that learning to select attire appropriate to specific occasions and activities is a critical factor in the total educational process. Understanding and employing the Hampton University Dress Code will improve the quality of one's life, contribute to optimum morale, and embellish the overall campus image. It also plays a major role in instilling a sense of integrity and an appreciation for values and ethics as students are propelled towards successful careers.

Students will be denied admission to various functions if their manner of dress is inappropriate. On this premise students at Hampton University are expected to dress neatly at all times. The following are examples of appropriate dress for various occasions:

1. Classroom, Cafeteria, Student Union and University Offices – causal attire that is neat and modest.
2. Formal programs in Ogden Hall, the Convocation Center, the Student Center Ballroom, the Little Theater and the Memorial Chapel – event appropriate attire as required by the event announcement.
3. Interviews – Business attire.
4. Social/Recreational activities, Residence hall lounges (during visitation hours) – casual attire that is neat and modest.
5. Balls, Galas, and Cabarets – formal, semi-formal and after five attire, respectively.

Quality Enhancement Plan (QEP): From These Roots ... A Foundation for Life: Mathematics and Financial Literacy

Examples of inappropriate dress and/or appearance include but not limited to:

1. Do-rags, stocking caps, skullcaps and bandannas are prohibited at all times on the campus of Hampton University (except in the privacy of the student's living quarters).
2. Head coverings and hoods for men in any building.
3. Baseball caps and hoods for women in any building.
 - a. This policy item does not apply to headgear considered as a part of religious or cultural dress.
4. Midriffs or halters, mesh, netted shirts, tube tops or cutoff tee shirts in classrooms, cafeteria, Student Union and offices;
5. Bare feet;
6. Short shirts;
7. Shorts, all types of jeans at programs dictating professional or formal attire, such as Musical Arts, Fall Convocation, Founder's Day, and Commencement;
8. Clothing with derogatory, offensive and/or lewd message either in words or pictures;
9. Men's undershirts of any color worn outside of the private living quarters of the residence halls. However, sports jerseys may be worn over a conventional tee-shirt.

Procedure for Cultural or Religious Coverings

1. Students seeking approval to wear headgear as an expression or religious or cultural dress may make a written request for a review through the Office of the Chaplain.
2. The Chaplain will forward his recommendation the Dean of Students for final approval.
3. Students that are approved will then have their new ID card picture taken by University Police with the headgear being worn.

All administrative, faculty and support staff members will be expected to monitor student behavior applicable to this dress code and report any such disregard or violations to the Offices of the Dean or Men, or Dean of Women for the attention of the Dean of Students.

CODE OF CONDUCT

Joining the Hampton Family is an honor and requires each individual to uphold the policies, regulations, and guidelines established for students, faculty, administration, professional and other employees, and the laws of the Commonwealth of Virginia. Each member is required to adhere to and conform to the instructions and guidance of the leadership of his/her respective area. Therefore, the following are expected of each member of the Hampton Family:

1. To respect himself or herself.
2. To respect the dignity, feelings, worth, and values of others.
3. To respect the rights and property of others and to discourage vandalism and theft.
4. To prohibit discrimination, while striving to learn from differences in people, ideas, and opinions.
5. To practice personal, professional, and academic integrity, and to discourage all forms of dishonesty, plagiarism, deceit, and disloyalty to the Code of Conduct.

Quality Enhancement Plan (QEP): From These Roots ... A Foundation for Life: Mathematics and Financial Literacy

6. To foster a personal professional work ethic within the Hampton University Family.
7. To foster an open, fair, and caring environment.
8. To be fully responsible for upholding the Hampton University Code.

Students with disabilities which require accommodations should (1) register with the Office of Testing Services and 504 Compliance to provide documentation and (2) bring the necessary information indicating the need for accommodation and what type of accommodation is needed. This should be done during the first week of classes or as soon as the student receives the information. If the instructor is not notified in a timely manner, retroactive accommodations may not be provided.

DISCLAIMER

This syllabus is intended to give the student guidance in what may be covered during the semester and will be followed as closely as possible. However, the professor reserves the right to modify, supplement and make changes as course needs arise.

Quality Enhancement Plan (QEP): From These Roots ... A Foundation for Life: Mathematics and Financial Literacy

Hampton University Scoring Rubric

The Hampton University Advisory Council of the Writing Program has approved and recommended the use of the scoring rubric as a guide for evaluating student-writing performance across the curriculum.

6

A paper in this category:

- States purpose (e.g., position or thesis) insightfully, clearly and effectively
- Provide thorough, significant development with substantial depth and persuasively marshals support for position
- Demonstrates a focused, coherent, and logical pattern of organization
- Displays a high level of audience awareness
- Use disciplinary facts critically and effectively
- Has support control of diction, sentence structure, and syntactic variety, but may have a few minor flaws in grammar, usage, punctuation, or spelling
- Documents sources consistently and correctly using a style appropriate to the discipline

5

A paper in this category:

- States purpose (e.g., position or thesis) clearly and effectively
- Provide development with some depth and complexity of thought and supports position convincingly
- Demonstrates effect pattern of organization
- Displays a clear sense of audience awareness
- Use disciplinary facts effectively
- Has good control of diction, sentence structure, and syntactic variety, but may have a few minor errors in grammar, usage, punctuation, or spelling
- Documents sources correctly using a style appropriate to the discipline

4

A paper in this category:

- States purpose (e.g., position or thesis) adequately
- Provides competent development with little evidence of complexity of thought
- Demonstrates an adequate pattern of organization
- Displays some degree of audience awareness
- Uses disciplinary facts adequately
- Has adequate control of diction, sentence structure, and syntactic variety, but may have some error in grammar, usage, punctuation, or spelling
- Documents sources adequately using a style appropriate to the discipline

3

Quality Enhancement Plan (QEP): From These Roots ... A Foundation for Life: Mathematics and Financial Literacy

A paper in this category:

- States purpose (e.g., position or thesis) but with varying degree of clarity
- Provides some development for most ideas
- Demonstrates some pattern of organization, but with some lapses from the pattern
- Displays uneven audience awareness
- Uses some disciplinary facts
- Has some control of diction, sentence structure, and syntactic variety, but may have frequent error in grammar, usage punctuation, or spelling
- Documents sources using a style appropriate to the discipline, but may have errors.

2

A paper in this category:

- States purpose (e.g., position or thesis) unclearly
- Provides inadequate development of thesis
- Demonstrates inconsistent pattern of organization
- Displays very little audience awareness
- Uses disciplinary facts ineffectively
- Has little control of diction, sentence structure, and syntactic variety, and may have a pattern of errors in grammar, usage, punctuation, or spelling
- Acknowledges sources but does not document them using a style appropriate to the discipline

1

A paper in this category:

- Fails to state purpose (e.g., position or thesis)
- Fails to develop most ideas
- Lacks a pattern of organization
- Displays no audience awareness
- Use few or no disciplinary facts
- Lacks control of diction, sentence structure, and syntactic variety, with a pattern of errors in grammar, usage, punctuation, or spelling
- Fails to document or acknowledge sources

Quality Enhancement Plan (QEP): From These Roots ... A Foundation for Life: Mathematics and Financial Literacy

Mapping to NSTISSI 4012 Standard

	FUNCTION FOUR ENSURE ESTABLISHMENT OF SECURITY CONTROLS	
B.	ACCESS	
1	Access Controls	
	Define manual/automated access controls	X
	Explain the importance of manual/automated access controls	X
2	Access Privileges	
	Explain the importance of access privileges	X
3	Discretionary Access Controls	
	Discuss discretionary access controls	X
	Explain the importance of discretionary access controls	X
4	Mandatory Access Controls	
	Define mandatory access controls	X
	Explain the importance of mandatory access controls A10 ANNEX A to CNSSI No. 4012	X
5	Biometrics/Biometric Policies	
	Explain biometric policies	X
6	Separation of Duties	
	Define the need to ensure separation of duties where necessary	X
	Explain the importance of the need to ensure separation of duties where necessary	X
7	Need-To-Know Controls	
	Define need to know controls	X
	Explain the importance of need to know controls	X
	FUNCTION TEN ASSESS NETWORK SECURITY	X

Quality Enhancement Plan (QEP): From These Roots ... A Foundation for Life: Mathematics and Financial Literacy

	Ensure that when classified/sensitive information is exchanged between IS or networks (internal or external), the content of this communication is protected from unauthorized observation, manipulation, or denial	
1	Connectivity	
	Discuss connected organizations	X
	Discuss connectivity involved in communications	X
	Explain the importance of connectivity involved in communications	X
2	Emissions Security (EMSEC) and TEMPEST	
	Define TEMPEST requirements	X
	Discuss threats from Emissions Security (EMSEC)	X
	Discuss threats from TEMPEST failures	X
	Explain the importance of the threats from Emissions Security (EMSEC)	X
	Explain the importance of the threats from TEMPEST failures.	X
3	Wireless Technology	
	Discuss electronic emanations	X
	Discuss threats from electronic emanations	X
	Explain the importance of wireless technology	X
	Explain the risks associated with portable wireless systems, viz., PDAs, etc.	X
	Explain the importance of vulnerabilities associated with connected systems wireless technology	X