CSC 484 Systems Security Administration, Management, and Certification

Instructor: Office: Telephone:

Office Hours:

E-Mail:

Course Description: Outlines the principles of systems security administration, management, and certification. Provisioning, procurement and installation of network, hardware and software systems for mission critical enterprises. System configuration and maintenance. Incident handling and response. Facilities Management. Contingency Plans. Law, standards of contract. Operations Management. System certification, testing and validation. Prerequisite: CSC 382 or Consent of the Chair.

Course Objectives: This course focuses on teaching and training students to be able to describe and apply the appropriate actions to manage and administrate the Information Systems in a secure manner, as well as be able to perform the comprehensive multidiscipline assessment of the technical and non-technical security features of an information system. After completing the courses, students would be able to

- Describe and apply the appropriate actions to manage and administer the Information System(s) in a secure manner.
- Describe Information Assurance regulations, policies, and guidelines.
- Ensure the information systems is operated, used, maintained, and disposed of in accordance with security policies and practices.
- Ensure users and system support personnel have the required security clearances, authorization, and are familiar with internal security practices.
- Evaluate known vulnerabilities to ascertain if additional safeguards are needed.
- Ensure the information system is accredited and certified.

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

- Describe and apply the appropriate actions to manage and administer the Information System(s) in a secure manner.
- Describe Information Assurance regulations, policies, and guidelines.
- Ensure the information systems is operated, used, maintained, and disposed of in accordance with security policies and practices.
- Ensure users and system support personnel have the required security clearances, authorization, and are familiar with internal security practices.
- Evaluate known vulnerabilities to ascertain if additional safeguards are needed.
- Ensure the information system is accredited and certified.

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

- Security Administration (6 hours)
- Security Architecture and Design (3 hours)
Quality Enhancement Plan (QEP): From These Roots … A Foundation for Life: Mathematics and Financial Literacy

- Security Technology (3 hours)
- Security Personnel (3 hours)
- Business Continuity Planning and Disaster Recovery (6 hours)
- Legal, Regulation, Compliance, and Investigations (6 hours)
- Certification and Accreditation (6 hours)
- Laboratory (12 hours)

*Mapping to CNSSI 4012 can be found here.*

Textbooks:


Supplemental Materials (SM):

- SM-2: NCSC-TG-029: Introduction to Certification and Accreditation
- SM-3: NSTISSI-1000 National Information Assurance Certification and Accreditation Process (NIACAP)
- SM-4: NIST SP 800-12: An Introduction to Computer Security: This NIST handbook
- SM-6: NASA Consolidation of Active Directory (NCAD) Compliance Waiver Form
- SM-7: NASA Mission Focus Review 137 Non-ODIN Waiver Form
- SM-8: NIST SP 800-61-rev1 Computer Security Incident Handling Guide
- SM-9: Army Regulation 25-2 Information Assurance
- SM-10: IETF RFC 3227 Guidelines for Evidence Collection and Archiving
- SM-11: Federal Records Act
- SM-12: Electronic Records Management Guideline
- SM-14: Federal Property and Administration Service Act
- SM-16: National Archives Act 1986
- SM-17: General Federal Records Act
- SM-19: The Freedom of Information Act
- SM-21: Public Law 107-347
- SM-22: Administrative Communications System - US Department of Education
Quality Enhancement Plan (QEP): From These Roots … A Foundation for Life: Mathematics and Financial Literacy

- SM-25: Delegation of Authority - signature authorization
- SM-26: Guidebook on Delegation of Authority
- SM-27: A Model for Information Assurance: An Integrated Approach

Course Outline:

<table>
<thead>
<tr>
<th>Week</th>
<th>Topics</th>
<th>Text chapters (see 4012 map for the details)</th>
<th>Supplemental Materials</th>
<th>Tests / Programs</th>
</tr>
</thead>
</table>
| 1    | 1. Security Administration  
|      | 1.1. Policy (SM-8, SM-22, SM-23, SM-24) | Krutz: Ch1, Ch2, Ch6, Ch9, Ch11, Ch12, Ch15, Appendix  
|      |                                             | Whitman: Ch4, Ch5, Ch10, Ch11, Ch12  
|      |                                                | Pfleeger: Ch1, Ch3, Ch4, Ch8 | SM-8, SM-22, SM-23, SM-24 |
| 2    | 1.2. Security Planning  
|      | 1.3. Risk Analysis/Risk Mitigation (SM-5)  
|      | 1.4. Organization Security Policies  
|      | 1.5. Physical Security | Krutz: Ch1, Ch10, Appendix  
|      |                                             | Whitman: Ch4, Ch5, Ch9 | SM-5  
|      |                                                | Pfleeger: Ch8 | HW-1 |
| 3    | 2. Security Architecture and Design  
|      | 2.1. Computer Architecture  
|      | 2.2. Protection Mechanism  
|      | 2.3. Assurance | Krutz: Ch5 | HW-2 |
| 4    | Laboratory | | | |
| 5    | 3. Security Technology  
|      | 3.1. Firewall  
|      | 3.2. VPN  
|      | 3.3. Intrusion Detection  
|      | 3.4. Access Control  
|      | 3.5. Others | Krutz: Ch2, Ch6, Ch7  
|      |                                             | Whitman: Ch4, Ch5 | HW-3 |
| 6    | 4. Security Personnel  
|      | 4.1. Roles & Responsibility  
|      | 4.2. Delegation of Authority (SM-4, SM-25, SM-26)  
|      | 4.3. Credentials of Information Security Professional  
|      | 4.4. Education, Training, and Awareness (SM-27)  
|      | 4.5. Information Ownership (SM-1, SM-2, SM-3) | Krutz: Ch1, Ch6  
|      |                                             | Whitman: Ch1, Ch5, Ch11 | SM-1, SM-2, SM-3, SM-4, SM-25, SM-26, SM-27 |
| 7    | Laboratory | | | |
| 8    | 5. Business Continuity Planning and Disaster Recovery  
|      |                                                | | HW-5 |
## Quality Enhancement Plan (QEP): From These Roots … A Foundation for Life: Mathematics and Financial Literacy

| 5.2. | Business Continuity Planning (SM-8, SM-9,) | Whitman: Ch5  
Pfleeger: Ch8 |
| 5.3. | Disaster Recovery (SM-8, SM-9, SM-28) | Krutz: Ch3, Ch8  
Whitman: Ch5  
Pfleeger: Ch8 |
| 5.4. | Incident Response (SM-8, SM-9, SM-28) | SM-8, SM-9, SM-28, SM-29 |
| 5.5. | Law enforcement interfaces/policies (SM-8, SM-9, SM-28) |  
| 5.6. | Reconstitution (SM-28, SM-29) | Krutz: Ch3, Ch8  
Whitman: Ch5  
Pfleeger: Ch8 |
| 5.7. | Restoration (SM-8, SM-9, SM-28) | Krutz: Ch3, Ch8  
Whitman: Ch5  
Pfleeger: Ch8 |

### 6. Legal, Regulation, Compliance, and Investigations

Whitman: Ch2, Ch3, Ch5  
Pfleeger: Ch9 |

### 7. Certification and Accreditation

| 7.1. | Understanding Certification and Accreditation (SM-1, SM-2, SM-3) | Krutz: Ch11, Ch14, Appendix  
Whitman: Ch1, Ch10 |
| 7.3. | Discuss the significance of NSTISSP No. 6 |  
| 7.4. | Approval to Operate (ATO)/Interim Approval to Operate |  
| 7.5. | Recertification (SM-2) |  


| 8.1. | Waive Policy to Continue Operation (SM-2, SM-4, SM-5, SM-6, SM-7) |  
| 8.2. | Certification Phase (SM-1, SM-3) |  
| 8.3. | Accreditation Phase (SM-1, SM-3) |  
| 8.4. | Role and Responsibility (SM-1, SM-2, SM-3) |  
| 8.5. | Information System Security Manager (ISSM) (SM-30) |  
| 8.6. | Information System Security Officer (ISSO) |  

### Laboratory

Pfleeger: Ch8 |
| 10. | Disaster Recovery (SM-8, SM-9, SM-28) | Krutz: Ch3, Ch8  
Whitman: Ch5  
Pfleeger: Ch8 |
| 12. | Law enforcement interfaces/policies (SM-8, SM-9, SM-28) | Krutz: Ch3, Ch8  
Whitman: Ch5  
Pfleeger: Ch8 |
| 13. | Reconstitution (SM-28, SM-29) | Krutz: Ch3, Ch8  
Whitman: Ch5  
Pfleeger: Ch8 |
| 14. | Restoration (SM-8, SM-9, SM-28) | Krutz: Ch3, Ch8  
Whitman: Ch5  
Pfleeger: Ch8 |
Whitman: Ch1, Ch10 |
| 17. | Certification Phase (SM-1, SM-3) |  
| 18. | Accreditation Phase (SM-1, SM-3) |  
| 19. | Role and Responsibility (SM-1, SM-2, SM-3) |  
| 20. | Information System Security Manager (ISSM) (SM-30) |  
| 21. | Information System Security Officer (ISSO) |  

### Important Dates:

**Exam 1:**  
**Exam 2:**  
**Final Exam:**

**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:

<table>
<thead>
<tr>
<th>Component</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Examine (2)</td>
<td>20 %</td>
</tr>
<tr>
<td>Homework (7)</td>
<td>40 %</td>
</tr>
<tr>
<td>Laboratory (4)</td>
<td>15%</td>
</tr>
<tr>
<td>Attendance &amp; participation</td>
<td>10 %</td>
</tr>
<tr>
<td>Ethics Paper</td>
<td>5 %</td>
</tr>
<tr>
<td>Final exam</td>
<td>10 %</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Grade</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>A+</td>
<td>98-100</td>
</tr>
<tr>
<td>A</td>
<td>94-97</td>
</tr>
<tr>
<td>A-</td>
<td>90-93</td>
</tr>
<tr>
<td>B+</td>
<td>88-89</td>
</tr>
</tbody>
</table>
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.
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.
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.
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.
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

10
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.

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

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
### Mapping to NSTISSI 4012 Standard

<table>
<thead>
<tr>
<th>FUNCTION ONE - GRANT FINAL ATO</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Granting final approval to operate an IS or network in a specified security mode</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### A. RESPONSIBILITIES

1. **Aspects of Security**

   **Explain the importance of SSM role in Information Assurance (IA)**

   Topic 4.1
   - Ch1, Pg. 26 (Roles and Responsibilities), Pg. 30 (RM Roles)
   - Ch1, Pg. 28-38 (Security Professionals and Organization)

2. **Accreditation**

   **Discuss accreditation**

   Topic 7.1
   - Ch11, Pg. 560 (Federal Information Processing Standard (FIPS) 102), Pg. 572 (What is Certification and Accreditation?), Appendix D, Pg. 977 (Implementation Phase - Security Accreditation)
   - Ch10, Pg. 453 (Certification Versus Accreditation)
   - NCSC-TG-029: Introduction to Certification and Accreditation

   **Discuss the certification process leading to successful accreditation**

   Topic 7.1
   - Ch11, Pg. 560 (Federal Information Processing Standard (FIPS) 102), Pg. 561 (DoD Information Technology Security Certification and Accreditation Process (DITSCAP)), Pg. 565 (The National Information Assurance Certification and Accreditation Process (NIACAP)), Pg. 567 (Defense Information Assurance Certification and Accreditation Process (DIACAP)),
   - Ch10, Pg. 453-465 (Information System Certification and Accreditation)

   **Explain the importance of accreditation**

   Topic 7.1
   - Ch11, Pg. 560 (Federal Information Processing Standard (FIPS) 102), Pg. 572 (What is Certification and Accreditation), Appendix D, Pg. 977 (Implementation Phase - Security Accreditation)
   - Ch10, Pg. 453-454 (Information System Certification and Accreditation)

   **Explain types of accreditation**

   Topic 7.1
   - Ch11, Pg. 566 (NIACAP Accreditation Types)
   - Ch10, Pg. 453-465 (Information System Certification and Accreditation)

   **Facilitate the certification process leading to successful accreditation**

   Topic 7.1
   - Ch11, Pg. 560 (Federal Information Processing Standard (FIPS) 102), Pg. 561 (DoD Information Technology Security Certification and Accreditation Process (DITSCAP)), Pg. 565 (The National Information Assurance Certification and Accreditation Process (NIACAP)), Pg. 567 (Defense Information Assurance Certification and Accreditation Process (DIACAP)),
   - Ch10, Pg. 453-465 (Information System Certification and Accreditation)
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page and Source</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Discuss the significance of NSTISSP No. 6</td>
<td>Ch11, Pg. 565-566 (NIACAP and NSTISSP #6)</td>
<td></td>
</tr>
<tr>
<td>2. APPROVAL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Approval to Operate (ATO)</td>
<td>Ch14, Pg. 647 (Authorization to Operate (ATO)), Pg. 656-657 (DIACAP Accreditation Phases)</td>
<td>NIST SP 800-37: Guide for Security Certification and Accreditation of Federal Information Systems</td>
</tr>
<tr>
<td>3. Interim Approval to Operate</td>
<td>Ch14, Pg. 647 (Interim Authorization to Operate (IATO)), Pg. 656-657 (DIACAP Accreditation Phases)</td>
<td>NIST SP 800-30: Risk Management Guide for Information Technology Systems</td>
</tr>
<tr>
<td>4. Recertification</td>
<td>Appendix D, Pg. 988-990 (Risk Mitigation), Appendix E, Pg. 1061 (Risk Mitigation)</td>
<td>NISTISSI-1000 National Information Assurance Certification and Accreditation Process (NIACAP)</td>
</tr>
<tr>
<td>6. Waive Policy to Continue Operation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Topic</td>
<td>Page/Section</td>
<td>Page/Section</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Discuss justification for waiver</td>
<td>Topic 7.7</td>
<td>Appendix D, Pg. 988-989 (Risk Mitigation), Appendix E, Pg. 1061 (Risk Mitigation)</td>
</tr>
<tr>
<td>Discuss risk mitigation strategies necessary to obtain waiver</td>
<td>Topic 7.7</td>
<td>Appendix D, Pg. 988-989 (Risk Mitigation), Appendix E, Pg. 1061 (Risk Mitigation)</td>
</tr>
<tr>
<td>Ensure risk assessment supports granting waiver</td>
<td>Topic 7.7</td>
<td>NSTISSI-1000 National Information Assurance Certification and Accreditation Process (NIACAP)</td>
</tr>
<tr>
<td>Discuss the contents of SSAA</td>
<td>Topic 7.6</td>
<td>Ch11, Pg. 563-564 (The System Security Authorization Agreement (SSAA))</td>
</tr>
</tbody>
</table>
### Quality Enhancement Plan (QEP): From These Roots … A Foundation for Life: Mathematics and Financial Literacy

<table>
<thead>
<tr>
<th>Function Three - Verify Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that each information system complies with the information assurance (IA) requirements.</td>
</tr>
</tbody>
</table>

#### A. LAWS RELATED TO INFORMATION ASSURANCE (IA) AND SECURITY

<table>
<thead>
<tr>
<th>1 Copyright Protection and Licensing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explain the importance of copyright protection.</td>
</tr>
</tbody>
</table>

**Topic 6.2**

- Ch9, Pg. 480 (Copyright)
- Ch2, Pg. 43-44 (Comprise to Intellectual Property), Ch3, Pg. 96-97 (U.S. Copyright Law)
- Ch9, Pg. 556-561 (Copyrights)

<table>
<thead>
<tr>
<th>2 Criminal Prosecution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explain the importance of criminal prosecution.</td>
</tr>
</tbody>
</table>

**Topic 6.3**

- Ch9, Pg. 586-587 (Why Computer Crime is Hard to Prosecute)
- NIST SP 800-61-rev1 Computer Security Incident Handling Guide
- Army Regulation 25-2 Information Assurance

<table>
<thead>
<tr>
<th>3 Due Diligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explain the importance of due diligence.</td>
</tr>
</tbody>
</table>

**Topic 6.4**

- Ch3, Pg. 357 (Due Care and Due Diligence), Ch9, Pg. 502-503 (Liability)
- Ch3, Pg. 89 (Organizational Liability and the Need for Counsel)

<table>
<thead>
<tr>
<th>4 Evidence Collection and Preservation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explain the importance of evidence collection.</td>
</tr>
</tbody>
</table>

**Topic 6.3**

- Ch9, Pg. 496-497 (Evidence)
- NIST SP 800-61-rev1 Computer Security Incident Handling Guide

<table>
<thead>
<tr>
<th>5 Due Diligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explain the importance of evidence preservation.</td>
</tr>
</tbody>
</table>

**Topic 6.3**

- Ch9, Pg. 495 (Preserved)
- IETF RFC 3227 Guidelines for Evidence Collection and Archiving
### 6 Laws Related To Information Assurance and Security

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Explain the importance of implications of Federal Managers Financial Integrity Act of 1982</td>
<td>Federal Managers Financial Integrity Act of 1982</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Explain the importance of implications of Federal Property and Administration Service Act</td>
<td>Federal Property and Administration Service Act</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Explain the importance of implications of National Archives and Records Act</td>
<td>National Archives Act 1986, General Federal Records Act</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Explain the importance of implications of the legal responsibilities of senior systems managers.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Explain the importance of implications of the Privacy Act</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Explain fraud, waste, and abuse

Topic 6.4

Ch6, Pg. 374 (Illegal Computer Operations and Intentional Attacks), Ch9, Pg. 474 (Fraud), Ch3, Pg. 190 (Network Attacks and Abuses), Ch9, Pg. 490 (1986 (amended in 1996 U.S. Computer Fraud and Abuse Act.)

Ch6, Pg. 587-588 (U.S. Computer Fraud and Abuse Act)

#### Ch6, Pg. 374

(1) **Illegal Computer Operations and Intentional Attacks**

- **Fraud**
  - Ch9, Pg. 474
  - Ch9, Pg. 490
  - Ch9, Pg. 491

- **Waste**
  - Ch6, Pg. 374

- **Abuse**
  - Ch9, Pg. 474
  - Ch6, Pg. 374
  - Ch3, Pg. 190

- **Intentional Attacks**
  - Ch9, Pg. 474
  - Ch9, Pg. 490
  - Ch9, Pg. 491

---

**Laws Related To Information Assurance and Security**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Explain the importance of implications of Federal Managers Financial Integrity Act of 1982</td>
<td>Federal Managers Financial Integrity Act of 1982</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Explain the importance of implications of Federal Property and Administration Service Act</td>
<td>Federal Property and Administration Service Act</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Explain the importance of implications of National Archives and Records Act</td>
<td>National Archives Act 1986, General Federal Records Act</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Explain the importance of implications of the legal responsibilities of senior systems managers.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Explain the importance of implications of the Privacy Act</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Ch6, Pg. 374**

(1) **Illegal Computer Operations and Intentional Attacks**

- **Fraud**
  - Ch9, Pg. 474
  - Ch9, Pg. 490
  - Ch9, Pg. 491

- **Waste**
  - Ch6, Pg. 374

- **Abuse**
  - Ch9, Pg. 474
  - Ch6, Pg. 374
  - Ch3, Pg. 190

- **Intentional Attacks**
  - Ch9, Pg. 474
  - Ch9, Pg. 490
  - Ch9, Pg. 491

---

**Ch9, Pg. 474**

(1) **Fraud**

- Ch9, Pg. 474
  - Ch9, Pg. 490
  - Ch9, Pg. 491

---

**Ch9, Pg. 490**

(1) **Fraud**

- Ch9, Pg. 474
  - Ch9, Pg. 490
  - Ch9, Pg. 491

---

**Ch9, Pg. 491**

(1) **Fraud**

- Ch9, Pg. 474
  - Ch9, Pg. 490
  - Ch9, Pg. 491

---

**Ch9, Pg. 490 (1986 (amended in 1996 U.S. Computer Fraud and Abuse Act.).)**

- Ch9, Pg. 474
  - Ch9, Pg. 490
  - Ch9, Pg. 491

---

**Ch9, Pg. 491 (1986 (amended in 1996 U.S. Computer Fraud and Abuse Act.).)**

- Ch9, Pg. 474
  - Ch9, Pg. 490
  - Ch9, Pg. 491

---

**Ch3, Pg. 190 (Network Attacks and Abuses).**

- Ch9, Pg. 474
  - Ch9, Pg. 490
  - Ch9, Pg. 491
<table>
<thead>
<tr>
<th>Topic</th>
<th>Description</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Legal and Liability Issues</td>
<td>Discuss implications of Public Law 107-347 regarding certification and accreditation Topic 6.2</td>
</tr>
<tr>
<td></td>
<td>Explain the importance of legal and liability issues as they apply to system and mission</td>
<td>Topic 6.4</td>
</tr>
<tr>
<td>8</td>
<td>Ethics</td>
<td>Discuss ethics</td>
</tr>
<tr>
<td><strong>B</strong></td>
<td>POLICY DIRECTION</td>
<td></td>
</tr>
<tr>
<td><strong>1</strong></td>
<td>Access Control Policies</td>
<td>Explain the importance of access control policies</td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>Administrative Security Policies And Procedures</td>
<td>Explain the importance of administrative security policies/procedures</td>
</tr>
<tr>
<td><strong>3</strong></td>
<td>Audit Trails and Logging Policies</td>
<td>Explain the importance of audit trail policy</td>
</tr>
<tr>
<td></td>
<td>Explain the importance of logging policies</td>
<td>Topic 1.1</td>
</tr>
<tr>
<td><strong>4</strong></td>
<td>Documentation Policies</td>
<td>Explain the importance of documentation policies</td>
</tr>
<tr>
<td><strong>5</strong></td>
<td>Evidence Collection and Preservation Policies</td>
<td>Explain the importance of evidence collection/preservation policies</td>
</tr>
<tr>
<td><strong>6</strong></td>
<td>Information Security Policy</td>
<td>Define information security policy</td>
</tr>
<tr>
<td></td>
<td>Explain the importance of information security policy</td>
<td>Topic 1.1</td>
</tr>
</tbody>
</table>
### Quality Enhancement Plan (QEP): From These Roots … A Foundation for Life: Mathematics and Financial Literacy

#### National Information Assurance (IA) Certification & Accreditation (C&A) Policy

**Topic 1.1** Ch11, Pg. 565-566 (NIACAP and NSTISSP #6) Ch10, Pg. 453-465 (Information Systems Security Certification and Accreditation)

#### Personnel Security Policies & Guidance

**Topic 1.1** Ch11, Pg. 20-25 (Security Policy Implementation), Pg. 25-26 (Roles and Responsibilities), Appendix B, Pg. 924 (Personnel Security)

#### Personnel Security Policies & Guidance

**Topic 1.1** Ch11, Pg. 470-502 (Positioning & Staffing the Security Function)

### SECURITY REQUIREMENTS

#### Access Authorization

**Topic 3.4** Ch2, Pg. 55-56 (Rationale) Ch5, Pg. 179 (Authorized Access and Usage of Equipment)

#### Background Investigations

**Topic 4.1** Ch6, Pg. 354 (Administrative Controls) Ch11, Pg. 493-494 (Background Checks)

#### Delegation of Authority

**Topic 4.2** Ch11, Pg. 471-492 (Positioning & Staffing the Security Function) Delegation of Authority - signature authorization Guidebook on Delegation of Authority

#### Education, Training, and Awareness

**Topic 4.4** Ch1, Pg. 42-45 (Security Awareness) Ch5, Pg. 206-209 (Security Education, Training, and Awareness Program) A Model for Information Assurance: An Integrated Approach

### FUNCTION FOUR ENSURE ESTABLISHMENT OF SECURITY CONTROLS

#### Access Controls

**Topic 3.4** Ch2, Pg. 55-61 (Access Control) Ch4, Pg. 141-142 (Access Control) Ch3, Pg. 194-204 (Control of Access to General Objects)

#### CONTINUITY OF OPERATIONS PLANNING

-
<table>
<thead>
<tr>
<th>1</th>
<th>Business Recovery</th>
<th>Define business recovery</th>
<th>Topic 5.2</th>
<th>Ch8, Pg. 435-446 (Business Continuity Planning)</th>
<th>Ch5, Pg. 209-237 (Continuity Strategies)</th>
<th>Army Regulation 25-2 Information Assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Explain the importance of business recovery</td>
<td>Topic 5.2</td>
<td>Ch8, Pg. 435-446 (Business Continuity Planning)</td>
<td>Ch5, Pg. 209-237 (Continuity Strategies)</td>
<td>NIST SP 800-61-rev1 Computer Security Incident Handling Guide</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Contingency/Continuity of Operations Planning</td>
<td>Explain the importance of contingency/continuity of operations planning</td>
<td>Topic 5.1</td>
<td>Ch8, Pg. 435-446 (Business Continuity Planning)</td>
<td>Ch5, Pg. 209-237 (Continuity Strategies)</td>
<td>NIST SP 800-61-rev1 Computer Security Incident Handling Guide</td>
</tr>
<tr>
<td></td>
<td>Ensure the establishment and testing of contingency/continuity of operations plans</td>
<td>Topic 5.1</td>
<td>Ch8, Pg. 435-446 (Business Continuity Planning)</td>
<td>Ch5, Pg. 209-237 (Continuity Strategies)</td>
<td>NIST SP 800-53-rev2-final Recommended Security Controls for Federal Information Systems</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Disaster Recovery</td>
<td>Explain the importance of disaster recovery</td>
<td>Topic 5.3</td>
<td>Ch8, Pg. 446-463 (Disaster Recovery Planning (DRP))</td>
<td>Ch5, Pg. 209-237 (Continuity Strategies)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Explain the importance of recovery plan</td>
<td>Topic 5.3</td>
<td>Ch8, Pg. 446-463 (Disaster Recovery Planning (DRP))</td>
<td>Ch5, Pg. 209-237 (Continuity Strategies)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ensure the establishment and testing of recovery plans</td>
<td>Topic 5.3</td>
<td>Ch8, Pg. 446-463 (Disaster Recovery Planning (DRP))</td>
<td>Ch5, Pg. 209-237 (Continuity Strategies)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Disaster Recovery Plan</td>
<td>Explain the importance of incident response policy</td>
<td>Topic 5.4</td>
<td>Ch3, Pg. 187-188 (Computer Incident Response Team)</td>
<td>Ch5, Pg. 209-237 (Continuity Strategies)</td>
<td>Ch8, Pg. 503-504 (Incident Response Plans)</td>
</tr>
<tr>
<td></td>
<td>Discuss law enforcement interfaces</td>
<td>Topic 5.5</td>
<td>Ch5, Pg. 235-237 (Law Enforcement Involvement)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Discuss law enforcement policies</td>
<td>Topic 5.5</td>
<td>Ch5, Pg. 235-237 (Law Enforcement Involvement)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Explain the importance of law enforcement interfaces</td>
<td>Topic 5.5</td>
<td>Ch5, Pg. 235-237 (Law Enforcement Involvement)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Incident response policies</td>
<td>Explain the importance of disaster recovery</td>
<td>Topic 5.3</td>
<td>Ch8, Pg. 446-463 (Disaster Recovery Planning (DRP))</td>
<td>Ch5, Pg. 209-237 (Continuity Strategies)</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Law enforcement interfaces/policies</td>
<td>Explain the importance of incident response policy</td>
<td>Topic 5.4</td>
<td>Ch3, Pg. 187-188 (Computer Incident Response Team)</td>
<td>Ch5, Pg. 209-237 (Continuity Strategies)</td>
<td>Ch8, Pg. 503-504 (Incident Response Plans)</td>
</tr>
<tr>
<td></td>
<td>Discuss law enforcement interfaces</td>
<td>Topic 5.5</td>
<td>Ch5, Pg. 235-237 (Law Enforcement Involvement)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Discuss law enforcement policies</td>
<td>Topic 5.5</td>
<td>Ch5, Pg. 235-237 (Law Enforcement Involvement)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Explain the importance of law enforcement interfaces</td>
<td>Topic 5.5</td>
<td>Ch5, Pg. 235-237 (Law Enforcement Involvement)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Reconstitution</td>
<td>Define principles of system reconstitution</td>
<td>Topic 5.6</td>
<td></td>
<td></td>
<td>GAO-08-1001 Information Security-Actions Needed to Better Protect Los Alamos National Laboratory's Unclassified Computer Network</td>
</tr>
<tr>
<td></td>
<td>Explain the importance of principles of system reconstitution</td>
<td>Topic 5.6</td>
<td></td>
<td></td>
<td>NIST SP 800-53-rev2-final Recommended Security Controls for Federal Information Systems</td>
<td></td>
</tr>
<tr>
<td>Function Five</td>
<td>Ensure Program Managers Define Security in Acquisitions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Explain the importance of restoration to continuity of operation A11 ANNEX A to CNSSI No. 4012</td>
<td>Topic 5.7</td>
<td>Ch8, Pg. 435-446 (Business Continuity Planning)</td>
<td>Ch5, Pg. 209-237 (Contingency Strategies)</td>
<td>Army Regulation 25-2 Information Assurance NIST SP 800-61 rev1 Computer Security Incident Handling Guide NIST SP 800-53 rev2- final Recommended Security Controls for Federal Information Systems</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2</th>
<th>System Security Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discuss system security architecture</td>
<td>Topic 2.1</td>
</tr>
</tbody>
</table>

| Explain how system security architecture supports continuity of operations CONOPS A12 ANNEX A to CNSSI No. 4012 | Topic 2.1 | Ch5, Pg. 198-199 (IETF Security Architecture), Pg. 201-206 (Design of Security Architecture) |

<table>
<thead>
<tr>
<th>Function Six</th>
<th>Assign Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigning Information Assurance (IA) responsibilities to the individuals reporting directly to the SSM</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1</th>
<th>Certification and Accreditation (C&amp;A)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discuss responsibilities associated with accreditation</td>
<td>Topic 7.10</td>
</tr>
</tbody>
</table>

| Discuss roles associated with certification | Topic 7.10 | Ch11, Pg. 573-577 (C&A Roles and Responsibilities) | Ch1, Pg. 28-38 Security Professionals and Organization |

| Explain importance of certification and accreditation (C&A) | Topic 7.1 | Ch11, Pg. 560-561 (Federal Information Processing Standard (FIPS) 102), Ch11, Pg. 572-573 (What is Certification and Accreditation?) |  |
## Quality Enhancement Plan (QEP): From These Roots … A Foundation for Life: Mathematics and Financial Literacy

<table>
<thead>
<tr>
<th>Topic</th>
<th>Section</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Facilitate the C&amp;A process</td>
<td>Ch11, Pg. 560 (Federal Information Processing Standard (FIPS) 102), Pg. 561 (DoD Information Technology Security Certification and Accreditation Process (DIACAP)), Pg. 565 (The National Information Assurance Certification and Accreditation Process (NIACAP)), Pg. 567 (Defense Information Assurance Certification and Accreditation Process (DIACAP)).</td>
</tr>
<tr>
<td>2</td>
<td>Information Ownership</td>
<td>Ch1, Pg. 24 (Roles and Responsibilities), Ch1, Pg. 573-577 (C&amp;A Roles and Responsibilities), Appendix D, Pg. 981 (Roles of Key Personnel in the Risk Management Process), Ch1, Pg. 29-30 (Data Ownership).</td>
</tr>
<tr>
<td>3</td>
<td>System Certifiers and Accreditors</td>
<td>Ch1, Pg. 30-38 (Overview of Risk Analysis), Ch12, Pg. 593-605 (Initial Risk Estimation), Appendix B, Pg. 929 (Risk), Ch10, Pg. 453-463 (Information System Security Certification and Accreditation).</td>
</tr>
<tr>
<td>4</td>
<td>Risk Analysts</td>
<td>Ch1, Pg. 30-38 (Overview of Risk Analysis).</td>
</tr>
<tr>
<td>5</td>
<td>Discuss risk as it applies to certification and accreditation</td>
<td>Ch1, Pg. 30-38 (Overview of Risk Analysis).</td>
</tr>
<tr>
<td>6</td>
<td>System Certifiers and Accreditors in risk mitigation</td>
<td>Appendix D, Pg. 988 (Risk Mitigation), Appendix E, Pg. 1061 (Risk Mitigation).</td>
</tr>
<tr>
<td>9</td>
<td>Define the role of Information Assurance Manager (ISSM)</td>
<td>NAVSO P-5239-04 Information Systems Security Manager (ISSM) Guidebook.</td>
</tr>
</tbody>
</table>