Instructor Notes

For

Information Security Planning: A Practical Approach

(Particularly for the Use of Case Study)Instructor Notes

# Introduction

Security Planning is meant to address multiple audiences well, including business and technical audiences and lower and upper-level students.

Lower-level courses can use the questions in the back of the chapter, with the instructor focusing on vocabulary, concepts and risks.

Upper-level courses with more mature students can use the rigor of the Security Workbook, optionally with the Health First case study. A longitudinal (semester-long) case study can involve either an industry of the student groups’ choosing or the Health First Doctor’s Office. When student projects choose an industry to study, the students complete the Security Workbook section associated with the chapter/lecture being covered to accomplish organizational security planning. The advantage of this option is that different student projects (covering various industries) will have varying concerns, which is interesting to cover in class. Case studies can be used as group homework or active learning exercise in class. Alternatively, students can use the Security Workbook for service-learning purposes, working with real organizational partners in the community. Optionally you may find it advantageous to start with the questions at the back of the chapters, for in-class discussions.

The Health First Case Study is an option where discussions are provided for each chapter-workbook exercise. Health First must adhere to advanced security regulation: in the U.S.: HIPAA/HITECH and in E.U.: GDPR. The advantage of this option is that organizational details are provided for students to work with.

I have used the chapter questions for a general education course, emphasizing the discovery of potential security problems, with less of a focus on detailed technical solutions. At our university, this course has also been taught to upper-level undergraduate computer science and graduate MBA and Computer Information Systems students, using a case study method.

# Using the Text for NSA & ACM CS Accreditation

***Addressing Educational Criteria***

For American universities wishing to achieve a National Security Agency (NSA) designation, this book attempts to address the Center of Academic Excellence Cyber Defense (CAE-CD) plan for 2021, including some Mandatory and Optional Knowledge Units (KU). While the book has not been submitted or approved by the NSA, the author has attempted to address each item in their list, to simplify the accrediting process. The book attempts to cover the entirety of the CAE-CD Nontechnical Core requirements. Often ‘Advanced’ sections cover more sophisticated topics beyond security planning. Very technical subjects (e.g., programming, networks, operating systems) are meant to be covered in other courses.

CAE-CD Knowledge Units addressed are shown in Table 1, indicating the chapters covered. The last category, Optional KUs at Introductory Level, introduces the vast majority of Topics in the KU but generally lacks one or more deeply technical exercises that are required as Outcomes. Some of the in-depth information required by NSA CAE knowledge units are covered in Advanced sections, which also provide more in depth information for more advanced organizations and practitioners. (NSA approval has not been obtained since NSA does not endorse textbooks.)

Since many required concepts are in the advanced sections and even in the questions, the author recommends using a digital version of the text to SEARCH for the required concepts, to ensure you cover them. Springer does not print indexes, since searches are easily done in digital versions.

*Table 1: NSA CAE-CD Chapter Mapping*

|  |  |
| --- | --- |
| **NSA CAE-CD Knowledge Units** | **Book Chapters** |
| Foundational: Cybersecurity Foundations | Ch. 1 Security Awareness,  Ch. 4 Risk,  Ch. 7 Info Security,  Ch 8 Network Security  Ch. 18 US Regulation  Ch. 20 Ethical Risk |
| Foundational: Cybersecurity Principles | Ch. 23 Software Requirements,  Ch. 8 Network Security |
| Technical Core: Network Defense | Ch. 1 Security Awareness,  Ch. 8 Network Security |
| Nontechnical Core: Cyber Threats, | Ch. 1 Security Awareness,  Ch. 8 Network Security,  Ch. 13 Incident Response  Ch. 18 US Regulation |
| Nontechnical Core: Cyber security Planning and Management | Ch. 6 Policy & Governance  Ch. 7 Information Security  Ch. 12 Personnel Security  Ch. 13 Incident Response  Ch. 5 Business Impact Analysis & Business Continuity |
| Nontechnical Core: Policy, Legal, Ethics, and Compliance | Ch. 3 PCI DSS  Ch. 18 US Regulation  Ch. 20 Ethical Risk  Ch. 8 Network Security  Ch. 16 Forensic Analysis (Advanced) |
| Nontechnical Core: Security Program Management | Ch. 6 Policy & Governance  Ch. 7 Information Security  Ch. 9 Physical Security  Ch. 10 Data Privacy  Ch. 12 Personnel Security  Ch. 13 Incident Response  Ch. 14 Metrics |
| Nontechnical Core: Security Risk Analysis | Ch. 4 Risk,  Ch. 10 Data Privacy |
| Optional KU: Basic Cyber Operations | Ch. 1 Security Awareness,  Ch. 8 Network Security,  Ch. 18 US Regulation |
| Optional KU: Cyber Crime\* | Ch. 1 Security Awareness,  Ch. 2 Fraud,  Ch. 17 EU GDPR,  Ch. 18 US Regulation,  Ch. 19 HIPAA |
| Optional KU: Cybersecurity Ethics | Ch. 18 US Regulation,  Ch. 20 Ethics of Risk |
| Optional KU: Fraud Prevention and Management, | Ch. 2 Fraud |
| Optional KU: IA Compliance, | Ch. 15 Audit,  Ch. 18 US Regulation,  Ch. 20 Ethics of Risk |
| Optional KU: IA Standards | Ch. 3 PCI-DSS,  Ch. 11 Advanced Networks (Cloud),  Ch. 18 US Regulation,  Ch. 19 HIPAA,  Ch. 21 Software Threats,  Ch. 22 Secure Software Processes |
| Optional KU: Life-Cycle Security | Ch. 21 Software Threats,  Ch. 22 Secure Software Processes,  Ch. 23 Software Requirements,  Ch. 6 Policy and Governance,  Ch. 12 Personnel Security,  Ch. 20 Ethics of Risk |
| Optional KU: Privacy | Ch. 7 Information Security,  Ch. 10 Data Privacy,  Ch. 8 Network Security,  Ch. 17 EU GDPR,  Ch. 18 US Regulation, |
| Optional KU, Introductory: Cloud Computing | Ch. 11 Advanced Networks |
| Optional KU, Introductory: Digital Forensics | Ch. 16 Forensic Analysis,  Ch. 2 Fraud,  Ch. 10 Data Privacy,  Ch. 13 Incident Response |
| Optional KU, Introductory: Software Assurance | Ch. 21 Software Threats,  Ch. 22 Secure Software Processes,  Ch. 23 Software Requirements |
| Optional KU, Introductory: Secure Programming Practices | Ch. 21 Software Threats,  Ch. 23 Software Requirements |
| Optional KU, Introductory: IA Architectures | Ch. 8 Network Security,  Ch. 7 Information Security (w. Section 3 header)  Ch. 9 Physical Security |

The text also meets most of the 2013 ACM Information Assurance and Security “Core” requirements for Computer Science, including Foundational Concepts, Principles of Secure Design, Defensive Programming, Threats and Attacks, and some of Network Security. Addressed electives include Security Policy, Secure S/W Engineering, and most of Web Security. Adherence to KUs is not fully accomplished when sections are marked with a \*, since some topics or programming projects may be missing.

*Table 2. ACM IAS Requirements*

|  |  |
| --- | --- |
| ACM Computer Science  Information Assurance and Security “Core” | Chapters |
| IAS/Foundational Concepts in Security | Ch. 1 Security Awareness,  Ch. 7 Information Security. |
| IAS/Principles of Secure Design | Ch. 7 Information Security,  Ch. 21 Software Threats,  Ch. 22 Secure Software Processes,  Ch. 23 Software Requirements |
| IAS/Defensive Programming\* | Ch. 21 Software Threats,  Ch. 22 Secure Software Processes. |
| IAS/Threats and Attacks | Ch. 1 Security Awareness,  Ch. 2 Fraud,  Ch. 8 Network Security,  Ch. 10 Data Privacy |
| IAS/Network Security\* | Ch. 8 Network Security,  Ch. 11 Advanced Networks |
| IAS/Web Security\* | Ch. 21 Software Threats,  Ch. 7 Information Security,  Ch. 8 Network Security. |
| IAS/Security Policy | Ch. 1 Security Awareness,  Ch. 5 Business Impact Analysis & Business Continuity,  Ch. 7 Information Security,  Ch. 10 Data Privacy,  Ch. 11 Advanced Networks |
| IAS/Secure Software Engineering | Ch. 21 Software Threats,  Ch. 22 Secure Software Processes,  Ch. 23 Software Requirements |

Finally, much of this text is derived from ISACA’s Certified Information Systems Auditor® (CISA) and Certified Information Security Manager® (CISM) study guides related to security. Other parts of these guides are generally covered by other courses, such as project management, networking, and software engineering. Students may pass these exams with additional study, particularly using ISACA’s CISA or CISM question disks.

# Introduction to the Case Study

In the US, many doctor’s offices or clinics are considered small businesses and must also adhere to federal laws governing privacy and security of patient information including the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its related security and privacy rules. The Health First Case Study was developed as a single case study in that the same organization is presented across the multiple challenges that are introduced. At the same time the specific challenges are presented as small case studies within the same organization and may be used separately or as a whole.

To help lead students through the case studies, a Security Workbook has been developed, which guides small businesses through the process of organizing a security program. The Security Workbook provides a procedure for building security plans for a generic small business. In combination, the Health First Case Study and Security Workbook introduce students to a realistic organizational setting.

The Security Workbook is portable and useful for graduates, since it has been used in a class setting with not-for-profits.

An overview of the documents available for a case study include:

* **Security Workbook:** Design security for the organization
* **Software Security Plan:** Design security for an organizational database (software design)
* **Health First Case Study:** A case study story based on a medical office for students to apply to the Security Workbook and Software Security Plan
* **Health First Database Security Plan**: The Software Security Plan, but with Health First within the name.
* **Health First Requirements:** The description of a hypothetical medical database for use with the Health First Case Study.

## Using the Health First Case Study

The Health First Case Study provides a number of assignments that may be taught as an active learning exercise in class, or as a homework assignment. The associated document for organizational planning is the Security Workbook.

For computer science students interested in software development, optional Secure Software assignments within the Health First Case Study relate to students designing security for a database for use at a doctors’ office. These assignments are generally longer and are done as homework. Students submit their software designs within the Health First Database Security Plan. A Health First Requirements Document describes a pre-existing medical database, for which students are designing security.

### In-Class Active Learning Exercise

PowerPoint lectures may be given in the first half of a 3-hour face-to-face class, while the second half is the active learning exercise. The lectures have been enhanced to include appropriate example tables from the Security Workbook, for a University application. The examples help students to observe how tables are properly used, and may provide ideas for their solution (or not). The text book and instructor lecture notes are available to students during the active-learning exercise.

During the active learning exercise, students may move to a computer room where they can edit the Security Workbook (or Security Plan for secure software designs) directly onto a computer. Students are grouped into 3-4 person teams, and each team is provided a computer. All students should be able to see the display, so students should be positioned arounds computers for the best display.

The instructor may provide each student with the 2-3 pages of the specific case study exercise, or students can imagine working with a particular industry of their choosing, independently. The Workbook is retained on the computer, so that students may add to the Workbook each week. The instructor can separate out each pertinent Workbook chapter, or can indicate which chapter in the Workbook students should work with.

When working with the Health First Case Study, the beginning of each case study chapter indicates the corresponding section in the Workbook to work with. The case study has subdivided headings to indicate the conversations for each subsection of the appropriate chapter in the Workbook. Students may start the case study by having students select specific roles to read, so each role is read by a different student. Most case studies have 4 roles, so there would normally be 4 readers. This has the advantage that students get to play the role of the IT person, versus a doctor or medical administrator. It also starts out the case study with students actively talking, and not silently reading (or being confused). If the case study is read out loud in front of the whole class, it enables the instructor the opportunity to start asking questions for class discussion, and getting initial ideas in play.

After the case study is being actively discussed per group, the instructor may see that some groups are too quiet or going in the wrong direction. It is helpful to guide the students by asking them where they are. Rarely, it may make sense to move people between groups, if some groups are not making sufficient progress or are not getting along. At the end of the class, the instructor can ask the class or specific teams to contribute parts of their solutions, particularly if they had brilliant ideas that should be shared, and/or can discuss the solution provided by the case study web site.

For active learning, students may be given credit for participating. If students miss the active learning exercise, they can submit it as homework. Due to the time constraints, perfect solutions may not occur during the lab time. However, having students think about the solution, and observe a good solution, helps them to assimilate the material. Often students come up with brilliant ideas which have been incorporated into the solution.

For many of the case studies, it is important that the appropriate regulation (e.g., HIPAA or GDPR) lecture has previously been given, and that the regulatory lecture notes are also available to students. The regulatory lecture copies are retained for reference in the teaching lab, and may be distributed at the beginning of each lab, when this material is important.

### Homework or Online Course

Because workbook assignments may overflow the class time, it may be useful to start the student groups working during class time, but expect the work to be submitted later as homework. This has the advantage of enabling the instructor to monitor direction and intervene in class if necessary, but expecting quality and complete work as an end product.

### Tips for Success in Working with the Case Study

Two goals of leading a longitudinal walkthrough case study is to ensure students are actively engaged, and that students are not confused. Leading the case study the right way can get students off to a quick and confident start. Many of these recommendations are from our observation of student behavior, and help to make running the labs easier. There were fewer questions, and students are busy right from the lab start.

**Start focused and easy**. The first case study is always confusing to the students. It should be very easy, to build comfort and confidence in working with a case study. Early case studies should focus on that week’s lecture materials. Toward the end of the semester, the focus can be more general and complex (integrating multiple concepts). The two easiest case studies are: *Fraud Combatting Social Engineering* or *Developing a Code of Ethics*. I start them as one class exercise with out-loud readers, not as group exercises.

**Give students only the materials they need**. One instructor told me that when he provides the full case study and full workbook, students get lost as to where they should be working. I provide a paper copy of the case lab separately (not as a full document), but provide students the full Workbook to edit directly and electronically. I also keep binders of relevant information in the lab and distribute one per group, but only when necessary: e.g., HIPAA lecture and Requirements Document. Except for the first week, there is little confusion.

**Explain complex material well**. The lecture is important to help guide students. Also, at the end of each lecture is directions for the assignment, showing examples. Use the extra slides at the end of the PowerPoint to simplify and review the materials.

**Provide easily-accessible details and examples**. The lecture and newly written text provide an example education-related case study solution for many of the Workbook case study tables. Provide details of your lecture on-line and encourage them to read the text first. I provide examples and details in the on-line PowerPoint lecture and text, and have observed that students referred to these examples.

**Explain that case studies have multiple correct answers**. ‘Authentic’ problems have increased complexity, which undergraduates are uncomfortable with. Since time in the lab is too short to develop a perfect answer, you may have each student team contribute part of their answer at the end of each lab. This way, the best ideas are highlighted. Students do not feel they need to have completed the full correct answer. The instructor may show a complete answer, but explains that multiple correct answers exist, and that the demo answer has been improved from previous student teams.

**Help international students**. Providing a dictionary of technical vocabulary with translations from English to student languages received positive comments on weekly evaluations.

### Can I order topics out-of-order?

Yes if you are careful.

For the security professional or service-learning educator, some chapters can be read and performed out of order (or in order of reader priority). The prerequisite understanding is always described at the beginning of each section and the beginning of each chapter.

The instructor may want to lecture in a particular order to match his/her textbook or for early introduction of topics for student service learning projects. The diagram below shows the potential ordering of the PowerPoint lectures. Topics are color-coded and stratified into levels. Green topics are lectures built from CISA/CISM materials. Red topics are non-ISACA areas, and include Fraud, HIPAA, and Secure Software topics. Blue topics are prerequisite courses/classes for specific lectures, and include introductions to programming.

The levels and arrows indicate prerequisites. Solid arrows are necessary prereqs, while dotted arrows can be done out-of-order, if the instructor is careful. The No Prereqs level indicates lectures with no prerequisites: Fraud, HIPAA and Security Awareness can be done at any time. However, either HIPAA and/or Security Awareness are prerequisites for Level 1 topics. Level 3 topics require Level 2 introduction first.

## Lecture Prerequisite Diagram and Table

The instructor may want to lecture in a particular order to match his/her textbook or for early introduction of topics for student service-learning projects. The diagram below shows the potential ordering of the PowerPoint lectures. Topics are color-coded and stratified into levels. Green topics are lectures built from CISA/CISM materials and usually work with the Workbook. Peach topics are non-ISACA areas, and include Fraud, HIPAA, and Secure Software topics. Blue topics relate to programming.

The levels and arrows indicate prerequisites. Solid arrows are necessary prerequisites, while dotted arrows can be done out-of-order, if the instructor is careful. The No Prerequisites level indicates lectures with no prerequisites: Security Awareness should be done first, but Fraud and HIPAA/GDPR can be done at any time. HIPAA/GDPR or other regulation is important for specific case studies. Level 3 topics require Level 2 introduction first.

No Prereqs

Regulation HIPAA or GDPR

(Program-ming)

Security Awareness

Fraud

Risk

Info Security

BIA/BC

Level 1

Security

Inspection

Software

Threats

Secure

S/W Process

Level 2

IT

Governance

Network

Security

Secure

Requirements

Level 3

Gover-nance

Physical Security

Incident

Response

IS

Audit

**Figure B1: Lecture Prerequisites**

In Table B below, the requirements for each case study exercise are described. One column describes the prerequisite lectures for the exercise. The Required Handouts column describes the notes and handouts that students should have accessible as they do the Case Study. Some cases can be associated with more than one lecture; the last column describes possible lectures.

Required handouts for each exercise are listed, and can be provided on-line or via paper notes. I make sure each group has access to a computer to update the Security Workbook or Database Security Plan directly.

For use with the Health First Case Study, it is helpful to also provide to each group a copy of the specific case study, HIPAA or GDPR lecture notes, and Health First Requirements.

**Table B1: Exercise Teaching Materials**

|  |  |  |  |
| --- | --- | --- | --- |
| **Exercise** | **Recommended Prerequisite Lecture** | **Required Handouts**  (Workbook = WB) | **Associated Lecture** |
| **Developing a Code of Ethics** | - | WB | Fraud or Ethical Risk |
| **Update Security Plan to include Segregation of Duties** | - | Security Plan,  Health First Req. | Fraud or Personnel Security or Secure Software |
| **Fraud: Combating Social Engineering** | - | - | Fraud or User Security Awareness |
| **HIPAA: Including Privacy Rule Adherence in Security Plan** | - | Security Plan,  Health First Req. | HIPAA |
| **Managing Risk** | HIPAA or GDPR lecture | HIPAA or GDPR Lecture, WB | Risk |
| **Addressing BIA and Business Continuity** | - | WB | Business Continuity |
| **Designing Information Security** | (Preferred but not necessary:) Business Continuity | WB, Health First Req. | Information Security |
| **Planning for Network Security** | Information Security and  Security Awareness | WB | Network Security |
| **Designing Physical Security** | Information Security,  HIPAA or GDPR | WB  Info Security Lecture, HIPAA or GDPR | Physical Security |
| **Planning for Incident Response** | Risk  Information Security  Network Security | WB  Software Assignment: Security Plan,  Requirements Doc. | Incident Response |
| **Organizing Personnel Security** | Business Continuity, Info security, Network security | WB | Personnel Security |
| **IT Governance: Planning for Strategic, Tactical, and Operational Security** | Risk,  Regulation: HIPAA, PCI DSS or GDPR | Governance Lecture  HIPAA or PCI DSS or GDPR Lecture | IT Governance |
| **Developing a Partial Audit Plan** | Regulation: HIPAA, PCI DSS or GDPR | WB,  Appendix D: Example Audit Plan | IS Audit |
| **Security Program Development: Editing a Policy Manual for HIPAA or GDPR or PCI DSS** | HIPAA or GDPR, Governing  (Info Security helpful) | HIPAA Lecture, WB | Best: Governing |
| **Defining Security Metrics** | Security Awareness, Risk, Information Security, Secure Software Threats, Network Security, Physical and Personnel Security | WB  Software Assignment: Security Plan, Requirements Doc. | Metrics |
| **Security Inspection: Extending Req. Preparation by Planning for HIPAA Security Rule** | HIPAA, Secure Software | Health First Requirements | Secure Software |
| **Software Req: Extending UML with MisUse Cases** | User Security Awareness,  Secure Software | Health First Requirements (optional) | Secure Software Design with UML |
| **Secure Software Design** | Secure Software,  Secure Software Design with UML,  Network Security | Secure Software Plan  Heath First Requirements | Extended homework assignment |