Stockholm University

Repetition, Questions and Examination coaching

COURSE: INFORMATION SECURITY IN ORGANIZATIONS

LEVEL: ADVANCED

Compulsory Literature = Study

- ISO/IEC 20000 Overview and Vocabulary (23p),
- ISO/IEC 27001 Information security management system (38p)
- FIPS 199 Information classification / Systems categorization(13p),
- FIPS 200 Information security requirements (17p)
- NIST 800-30 Risk Assessment (chapter 3 and Appendix D through I) (ca 40p)
- **Special case of ISO/IEC 27002 is marked as Reference, but compulsory to read these sections**:
  - Read: Pages i through 3, and then
  - Read: The FIRST security control with "objective", "control", "implementation guidance" and "other information" for each of the chapters 6-18, that is 6.1.1, 7.1.1, ... , 18.1.1.

- In total ca. 120 pages to Study (when not counting front matters etc.)
- The rest of the literature is marked as reference material

How to read the 100 pages

- Read for understanding, not for cramming.
- The questions on the exam will be of two kinds:
  - Some that ask for some facts, definitions, etc. that was directly presented in the course lectures or literature
  - Some that requires your understanding – not presented directly, e.g.
    - "Which would you ideally tackle first security controls or security requirements?"
- We have selected a very limited number of pages for reading so that you should be able to read and reflect.

Examination

WRITTEN EXAMINATION

Rules for examination 1/5

- Exam time: 2021-01-10 at 10-14 at the department
- The exam will be traditional onsite, requires registration in Daisy,
- The exam will consist of 50 short (one or two sentences) multiple choice exam questions, with four short answer alternatives.
- I have decided to give EXTRA TIME for ALL students to complete this exam. Instead of 2 hours, you will have 4 hours. The average time to complete the exam was lass than one hour last time, but this will vary.
- Please note that answering this exam does not require you to WRITE anything, you just tick a box!

Rules for examination 2/5

- Please note that the exam is not the same as last year (same format but not the same questions).
- The exam is done individually, so you may NOT look at each others answers.

Rules for examination 3/5

- Each question have four alternatives. Only one is correct and gives points. You must choose only ONE.
- IF you have no idea – take a chance – no deduction for wrong answer.
- If you do not know the answer:
  - Rule out those two who seems least likely
  - Then pick your answer randomly from the remaining two.

Rules for examination 4/5

- If the examiner can not see which alternative is chosen, 0 points will be given.
- For example, if you have marked two and partly erased on answer, this would give 0 points.
- The correct answer is given by
  1. Literature (only compulsory literature, not reference literature)
  2. Lecture slides
  3. What was said in the lectures
- In that order, if there is any inconsistency

Rules for examination 5/5

- The questions might contain more than one answer alternative that is somewhat correct.
- You need to pick the one that you deem as MOST correct.

Grading

- 50 questions
- 2 points each
- Max 100 p
  - A 90-100
  - B 80-89
  - C 70-79
  - D 60-69
  - E 55-59
  - Fx 50-54 (no need to resit exam, but new task)
  - F 00-49 (resit exam required)
- In essence, you need 25 correct answers to pass.

Time planning

- 5 mins per question
- If stuck, spend only 5 minutes then move forward
- In the end, look back for each of the uncertain ones.
- If more time left, double check!

Question example

- **Question 1**: The international standard ISO/IEC **27005** is mainly about?
  - Gaps
  - Risks
  - ISMS
  - Continuity

- Correct answer
- Where would you find this answer?
  - In ISO/IEC 27000
  - In Lecture 5

Your questions on the examination

- **Any questions?**

A look at the literature

- **NOTE: All of these documents are compulsary, all pages, however if you run out of time this is where you will find the most important material:**
  - **27000 – section 3 most important, 8 pages**
  - **27001 – section 1-10 most important, 9 pages**
  - **FIPS 199 – section 1-3 most important, 6 pages**
  - **FIPS 200 – section 1-4 most important, 4+ pages**
- **Only parts compulsary**
  - **SP800-30 – section 3 and Appendix D through I, ca 40 pages**
  - **Special case of ISO/IEC 27002 is marked as Reference, but compulsory to read these sections:**
    - Read: Pages i through 3, and then
    - Read: The FIRST security control with "objective", "control", "implementation guidance" and "other information" for each of the chapters 6-18, that is 6.1.1, 7.1.1, ... , 18.1.1.

Shall I take the next exam instead?

- **No! Take the first one even if you have little time to prepare.**
- **The next exam will not be only multiple choice**
- **Since you will be few left, I will make sure to have more open questions requiring written answers on the second exam.**
  - **The reason is the cost associated with developing a new multiple choice exam as it is very time consuming.**
  - **And since few left, we can spend more time in analysing each answer and have long answers.**
- **Sit the first exam!**

Course evaluation

- In Daisy
- Please answer