

Institutionen för Data- och Systemvetenskap
Stockholms Universitet

Written Examination 2022-01-15, 4,5 av 7,5 points

| | |
|--------------|---------------------------------------|
| Course: | SECORG |
| Course name: | Information Security in Organizations |
| Responsible: | Dr. Fredrik Blix |
| Time: | 2022-01-15, 1000-1400 (4 hours) |

Turn this page to start your examination.

All answers should be given on a separate answer sheet distributed with this exam:

We wish you good luck on your test!

Rules for examination

Respondents are allowed to bring one GENERAL English wordlist book. Instructions to exam proctors: Inspect each book to ensure that there are no notes relating to this exam inside the books.

ISO/IEC 27000 Questions

1) What is defined as “a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization’s information security to achieve business objectives”?

- a) Risk assessment process
- b) Information security management system (ISMS)**
- c) Information security policy document
- d) Monitoring and Measuring

2) Which of the following is *not* one of the “fundamental principles” that “also contribute to the successful implementation of an ISMS”?

- a) assignment of responsibility for information security
- b) incorporating management commitment and the interests of stakeholders
- c) security incorporated as an essential element of information networks and systems
- d) active prevention and detection of stakeholder deviations**

3) Information can be stored in many forms. Which forms are mentioned in ISO/IEC 27000?

- a) digital form
- b) material form
- c) digital and material forms
- d) digital and material forms as well as knowledge of the employees.**

4) Which term means “informed decision to take a particular risk”?

- a) Risk criteria
- b) Risk acceptance**
- c) Risk avoidance
- d) Risk analysis

5) The standard ISO/IEC 27003 is concerned with what?

- a) It contains an ISMS assessment methodology
- b) It provides guidance on the requirements of ISO/IEC 27001**
- c) It explains more in detail all the controls of ISO/IEC 27002
- d) Competence requirements for CISOs

ISO/IEC 27001 Questions

- 6) Is the ISMS described in ISO/IEC 27001 also intended to be useful in small organisations?
- a) No, only for 100 employees and over
 - b) No, only for 30 employees and over
 - c) Yes, the size of the organisation does not matter.**
 - d) Yes, but only requirements in sections 4-6 are applicable.
- 7) Is there a requirement in ISO/IEC 27001 that the information security policy shall be available as documented information?
- a) No, no requirement to document it at all
 - b) Yes, but only if determined by the organization as being necessary for the effectiveness of the ISMS
 - c) Yes, but only if required by one or more stakeholders
 - d) Yes, no matter what**
- 8) How are information security controls selected for implementation according to ISO/IEC 27001?
- a) All controls come straight from the risk assessment
 - b) Selected controls need to be compared with controls listed in Annex A**
 - c) Controls to be implemented are those listed in Annex A
 - d) The method for control selection is not prescribed
- 9) What could you expect to find in a document called "statement of applicability"?
- a) applicable controls and justification for these controls**
 - b) applicable risks and associated scenario descriptions
 - c) statements that are applicable to the ISMS
 - d) recent information security incidents
- 10) Interested parties may include *for example*:
- a) internal individuals and groups
 - b) external individuals and groups
 - c) both "a" and "b", internal and external individuals and groups**
 - d) none of the above

ISO/IEC 27002 Questions

11) What is this standard concerned with?

- a) **It contains security controls (security measures)**
- b) It contains requirements for information security management systems
- c) Both “a” and “b”
- d) None of the above

12) What is true regarding “control objectives” according to ISO/IEC 27002?

- a) They are mainly used to control information security objectives
- b) **They state what should be achieved by one or more controls**
- c) They are objectives that are used during incidents only
- d) They are only used for auditing the ISMS

13) “Segregation of duties” is a method for reducing the risk of accidental or deliberate misuse of an organization’s assets. What does it mean?

- a) To pay duty in two separate instalments
- b) That each person’s duties should be separable from the person
- c) That two persons should not perform the same duties
- d) **Segregated responsibilities to reduce opportunities to breach security**

14) Who should ensure that information assets are appropriately inventoried, classified and protected?

- a) **The asset owner**
- b) The CEO (Chief Executive Officer)
- c) The CISO (Chief Information Security Officer)
- d) The CDO (Chief Digital Officer)

15) What is the point of “information classification”?

- a) To ensure that all risks receive an appropriate level of treatment
- b) To ensure that all security controls are implemented
- c) It has the same meaning as risk assessment
- d) **To ensure that information receives an appropriate level of protection**

FIPS 199 Questions

16) What is true regarding the FIPS 199 security categorization scheme and its impact definition for *high* confidentiality impact”? “The unauthorized disclosure of information could be expected to have a

- a) “Limited” adverse effect
- b) “Serious” adverse effect
- c) “Severe or catastrophic” adverse effect**
- d) There is no definition of high confidentiality impact in FIPS 199

17) FIPS 199 establishes security categories for both information and information systems. The security categories are based on the potential ... ?

- a) risk for a security breach
- b) information regarding a security breach
- c) impact on an organization in case of security breach**
- d) impact and probability for a security breach

18) Categorise historic public information about Swedish kings in a royal archive, in accordance with the security categorization scheme?

- a) SC archive = {(confidentiality, HIGH), (integrity, LOW), (availability, MODERATE)}
- b) SC archive = {(confidentiality, LOW), (integrity, LOW), (availability, LOW)}
- c) SC archive = {(confidentiality, NA), (integrity, LOW), (availability, HIGH)}.
- d) SC archive = {(confidentiality, NA), (integrity, HIGH), (availability, LOW)}**

19) You have found both “contract” and “administrative” information in the same information system, categorised as **SC** contract information = {(confidentiality, MODERATE), (integrity, MODERATE), (availability, LOW)} and **SC** administrative information = {(confidentiality, LOW), (integrity, LOW), (availability, LOW)}. Categorise the *information system* where both information types reside to ensure proper protection?

- a) {(confidentiality, MODERATE), (integrity, MODERATE), (availability, LOW)}.**
- b) {(confidentiality, HIGH), (integrity, MODERATE), (availability, LOW)}.
- c) {(confidentiality, MODERATE), (integrity, HIGH), (availability, HIGH)}.
- d) {(confidentiality, LOW), (integrity, LOW), (availability, HIGH)}.

20) Is potential impact of a security breach on individuals considered in FIPS 199?

- a) No, it is only concerned with national security and societal functions
- b) No, it is only concerned with organisations
- c) Yes, this is explicitly stated in the text**
- d) Yes, not spelled out in the text – but implied

FIPS 200 Questions

- 21) What is a low-impact information system according to FIPS 200?
- a) A system with low confidentiality impact levels
 - b) A system with low availability impact levels
 - c) A system with low integrity impact levels
 - d) A system with low impact levels on all aspects listed above**
- 22) In using FIPS 199 and FIPS 200, which should be done first – determination of information system impact levels or the selection of appropriate security controls?
- a) Determination of the “impact levels”**
 - b) Selection of the “security controls”
 - c) It depends on the business context
 - d) It does not matter which one is done first
- 23) How shall organisations meet the stated “minimum security requirements” according to FIPS 200?
- a) They just need to comply to them as they are written in FIPS 200
 - b) They shall remove the ones that are not needed and comply to the rest
 - c) They shall select appropriate controls in another document**
 - d) They do not need to meet them at all
- 24) Which term in FIPS 200 refers to “The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability”?
- a) A threat
 - b) A threat intention
 - c) A threat source**
 - d) A technical control
- 25) What is a high-impact system in FIPS 200? It is an information system in which ...
- a) at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high**
 - b) at least two security objectives are assigned a potential impact value of high
 - c) all three security objectives are assigned a potential impact value of high
 - d) None of the above

NIST SP 800-30 Questions

26) According to SP 800-30, *preparing* for a risk assessment includes all of the following tasks, *except* which one?:

- a) Identify the sources of information (to be used as inputs to the assessment)
- b) Identify the purpose of the assessment
- c) Identify the scope of the assessment
- d) **Identify the requirements and risks associated with the assessment**

27) SP 800-30 asks us to consider *predisposing conditions*. What does it mean?

- a) **Condition that contributes to the likelihood that a threat materialises**
- b) **Condition that contributes to the probability that a threat materialises**
- c) Factor that comes before the threat itself
- d) Conditions under which one should dispose of confidential information

28) “Tier 1”, “tier 2” and “tier 3” are used to signify what in SP 800-30?

- a) Risk levels
- b) Security categorisation levels
- c) **Organizational, Business process and Information Systems levels**
- d) Impact levels

29) Adversarial, accidental and environmental are examples of what?

- a) Risks
- b) **Threat sources**
- c) Threat events
- d) Impacts

30) Risk is a “measure of the extent to which an entity is threatened by a potential circumstance or event”, and is typically a function of (what)?:

- a) a threat event
- b) the likelihood
- c) **the likelihood and the impact**
- d) the likelihood and the threat event

Cyber Resilience Questions

31) What is supposed to be able to “continuously deliver its intended outcome despite adverse cyber events”, in a cyber resilience context?

- a) A technical information system
- b) A business process
- c) A nation
- d) **Potentially all of the above**

32) What is an “adverse cyber event” (in the context of Cyber Resilience)?

- a) Only adversarial events (e.g. hacker attack)
- b) All negative events that may happen to the business
- c) **All events that negatively impact the availability, integrity or confidentiality of networked IT systems and associated information and services**
- d) Only “acts of God” are considered adverse cyber events

33) What does *resilience* in general have to do with the *corona virus outbreak*?

- a) The corona virus uses the *same* transmission method as a computer virus
- b) **Society must make an effort to continuously deliver its intended outcome even in the face of serious adversity, such as the corona virus**
- c) Both “a” and “b”
- d) None of the above – there is no connection between resilience and the outbreak

34) It is said that resilient systems should be designed to be able to fail in a controlled way, rather than being designed to solely protect against failure. What is this design feature called?

- a) Failsafe
- b) **Safe-to-fail**
- c) Fail-to-safe
- d) Failsafe mode

35) Which of the following is most likely an “unintentional act of man”?

- a) **System down after failed update**
- b) Hacker attack against our system
- c) Distributed denial-of-service attack against our system
- d) Fire

Other Questions

36) Which of these terms refers to “a set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives” is?

- a) Information security policy
- b) Management system**
- c) International standards
- d) Business processes

37) Which document makes the ISMS visible?

- a) Policy
- b) Procedures
- c) Guidelines
- d) All of the above**

38) In which industry sector is HIPAA used?

- a) Healthcare**
- b) Telecom
- c) Algotrading
- d) Financial services

39) What is the main drawback with letting information classification for a given asset completely determine the selection of information security controls?

- a) It is illegal to do so
- b) It is very time consuming
- c) It gives the CISO too much power
- d) Important factors, e.g. risks, are overlooked**

40) Which of the following do you need to take into account when selecting appropriate technical and organisational measures to protect personal data in accordance with GDPR (EU General Data Protection Regulation)?

- a) The context and purpose of processing
- b) The cost of implementation
- c) The nature and scope of processing
- d) All of the above**

Other Questions

41) Which of the following may be an example of an *adversarial* threat source?

- a) Privileged insider
- b) Established hacking group
- c) **All – a, b and d are such examples**
- d) Competing business organisation

42) How can we ensure that *all* potentially relevant risks are analysed in our risk assessment?

- a) By using historical data
- b) By getting the risks from the risk register
- c) **We can not ensure that**
- d) By working systematically

43) What is one major difference between the definitions of "risk" in ISO/IEC 27001 and NIST SP 800-30?

- a) There are no major differences
- b) In 27001 risk can be only negative, in 800-30 risk can be both negative and positive
- c) **In 800-30 risk can be only negative, in 27001 risk can be both negative and positive**
- d) In 27001, risk is mainly based on likelihood – not impact as in 800-30.

44) In ISO/IEC 27002, chapter 10 is on "Cryptography". It contains only two controls, one is about "key management" and the other is about (what)?

- a) **Policy on the use of cryptographic controls**
- b) Policy on the use of Public Key Encryption PKE
- c) Public Key Infrastructure PKI
- d) Digital evidence

45) Is *network security management* covered in ISO/IEC 27002?

- a) No, you would have to look for other standards to handle that
- b) No, but there are other standards in the 27000-series of standards on that
- c) **Yes, there are some controls on that**
- d) No, that can not be standardized

Other Questions

- 46) Which of the following is a potential benefit of measuring information security?
- a) To prove progress in the work
 - b) Evidence of meeting requirements
 - c) To prove to external actors that external requirements are met
 - d) All of the above**
- 47) What is usually the meaning of “Asset Management” in information security?
- a) It refers to the people and companies who manage investments on behalf of others
 - b) It refers to identifying and protecting information- and IT-related assets**
 - c) It means identifying the root cause of an incident
 - d) It includes Protect, Defend, Comply, Assess
- 48) What is the “gap” in a “GAP-analysis”?
- a) There is no gap – GAP is an abbreviation
 - b) The gap between where we are and where we want to be**
 - c) The gap between us and the hackers
 - d) The gap between the different risk treatment options
- 49) Which of the following is an example of a tool that can be used for *technical vulnerability* analysis?
- a) Nessus
 - b) Qualys (QualysGuard)
 - c) OpenVAS
 - d) All of the above**
- 50) When managing information security in organisations, people should be viewed as (what)?
- a) Being assets
 - b) Being potential threat sources
 - c) Being part of the Security controls
 - d) All of the above**