1: **How should obsolete prototypes, models, and test items be disposed of?**

Domain: Information Security

2: **What qualifies something as a trade secret?**

Domain: Information Security

3: **What are three methods of sanitizing electronic media?**

Domain: Information Security

4: **What are the two primary aspects of recovery after an information loss?**

Domain: Information Security

5: **During which stage of a project is critical information most vulnerable?**

Domain: Information Security

6: **What is the difference between embedded and host-based systems?**

Domain: Information Security

7: **What three aspects of information must be protected?**

Domain: Information Security

8: **What are the five IS infrastructure management countermeasures?**

Domain: Information Security

2: **The information added value or benefit to the owner, the trade secret was specifically identified, and the owner provided a reasonable level of protection for the information**

IAP 1.5.4 p 24

1: **They should be destroyed so they can't be reverse engineered**

IAP 1.4.2 p 14

4: **Return to normal business operations ASAP and implement measures to prevent a recurrence**

IAP 1.7 p 30

3: **Overwriting, degaussing, physical destruction**

IAP 1.6.2 p 27

6: **Embedded systems** are typically programmed at the manufacturer and run proprietary or nonstandard operating systems, e.g. cameras, card readers, and video converters.

Host-based systems run on more standard operating systems such as Windows and Linux and are easier to change

IAP 2.5 p 73

5: **The intermediate phases**

IAP 1 Appendix D p 49

8: **Vulnerability and patch management, system monitoring and log review, IS security metrics, physical security of the IS infrastructure, IT staff training in information security**

IAP 3.1.6 p 91

7: **Confidentiality, integrity, availability**

IAP 2.3 p 69, IAP 3 85

9: What are the seven layers of the Open Systems Interconnect network model?

Domain: Information Security

10: What is the “A triad” of information security with regard to access control?

Domain: Information Security

11: What is an escalation of privilege attack?

Domain: Information Security

12: According to ISO 27002, which three elements of guidance should information security policies include, at a minimum?

Domain: Information Security

Domain: Information Security

Domain: Information Security

Domain: Information Security

Domain: Information Security

10: Authentication, authorization, auditing/accountability

IAP Figure 3-7 p 103

9: Physical, data link, network, transport, session, presentation, application

IAP 3.2.1 p 97

12: Definition of information security and its objectives/scope, statement of management intent, brief explanation of security policies/principles/standards important to the organization

IAP 3.5.2 p 141

11: When an email program is tricked into executing an email as if it were a program rather than text

SOP 3.2.1 p 48 Security Management 4.5.1 p 90