1. **What is management?** Management is the process of achieving objectives using a given set of resources. A manager is someone who works with and through other people by coordinating their work activities in order to accomplish organizational goals. There are differences between leadership and management. A leader influences employees so that they are willing to accomplish objectives, while a manager administers the resources of the organization. Managerial roles include informational role (collecting, processing, and using information), interpersonal role (interacting with superiors, subordinates, outside stakeholders), and decisional role (selecting from among alternative approaches, and resolving conflicts, dilemmas, or challenges) (Pages 2, 4, 5).

2. **What is POLC and how does it work?** POLC stands for Planning, Organizing, Leading, and Controlling. These are the principles of management categorized in the popular management theory, as opposed to the traditional management theory which uses the core principles of Planning, Organizing, Staffing, Directing, and Controlling (POSDC) (Page 6).

3. **What are the unique functions of InfoSec management known as "the six Ps"?** The six P's of Information Security Management are Planning, Policy, Programs, Protection, People, and Project Management. Planning in InfoSec management includes activities necessary to support the design, creation, and implementation of information security strategies. People are the most critical link in the information security program and managers must recognize the crucial role that people play in the information security program (Pages 16, 17, 18, 22).

4. **Why and how the project management is applied to security?** Project management is applied to security to integrate the disparate elements of a complex information security project. The PMBoK (Project Management Body of Knowledge) is considered the industry best practice for this. Information security is a process, not a project. Each element of an information security program must be managed as a project, forming a continuous series, or chain, of projects. Some aspects of information security are not project based but are managed processes (operations) such as monitoring internal/external environments, ongoing risk assessments, continuous vulnerability assessment (Pages 24, 27, 32).

5. **What is contingency planning and why is it important?** Contingency planning is the overall planning for unexpected events. It involves preparing for, detecting, reacting to, and recovering from events that threaten the security of information resources and assets. The main goal of contingency planning is the restoration to normal modes of operation with minimum cost and disruption to normal business activities after an unexpected event (Page 3).

6. **What are the three types of contingency plan and what are their respective usage context?** Incident Response Planning (IRP): This type of contingency planning is focused on preparing for, reacting to, and recovering from specific incidents that threaten the security or operation of the organization. These incidents could range from cyber attacks to equipment failures. Disaster Recovery Planning (DRP): This type of contingency planning is focused on recovering from major disruptions, such as natural disasters or significant security breaches. The goal is to restore operations as quickly and smoothly as possible after such a major event. Business Continuity Planning (BCP): This type of contingency planning is focused on ensuring that critical business functions can continue during and after a disaster. This often involves identifying critical functions and processes, and planning for how these can be maintained or quickly restored in the event of a disruption. These types of contingency planning are all important aspects of preparing for and responding to potential threats to an organization's information security and overall operations (Page 68).

7. **What roles do policies play in information security management?** Policies are the essential foundation of an effective information security program. The success of an information resources protection program depends on the policy generated, and on the attitude of management toward securing information on automated systems. The policy maker sets the tone and emphasis on the importance of information security (Page 4).

8. **What are the three types of policy? What are they about (what do they address)? Who will define these policies?** The three types of information security policy are:
    - Enterprise Information Security Program Policy (EISP): This policy sets the strategic direction, scope, and tone for all security efforts within the organization.
    - Issue-Specific Information Security Policies (ISSP): These policies often address specific areas of technol-

ogy, requiring frequent updates and having a more limited scope.
- Systems-Specific Policies (SysSP): These policies are often used as standards or procedures to be used when configuring or maintaining systems (Page 11).

9. **How to make policies effective? (develop, distribute, review, understand, agree, enforce)** For policies to be effective, they must be properly developed using industry-accepted practices, distributed or disseminated using all appropriate methods, reviewed or read by all employees, understood by all employees, formally agreed to by act or assertion, and uniformly applied and enforced. Effective policy is written at a reasonable reading level, and attempts to minimize technical jargon and management terminology (Pages 38, 44).

10. **What are the typical reporting structures in organisations of various sizes (very large, large, medium, small) and their advantages and limitations?**
    - Very Large Organizations: These organizations do a better job in the policy and resource management areas. However, only 1/3 of organizations handled incidents according to an Incident Response plan (Page 6).
    - Large Organizations: These organizations have 1,000 to 10,000 computers. Their security approach has often matured, integrating planning and policy into the organization's culture (Page 6).
    - Medium-Sized Organizations: These organizations have between 100 and 1000 computers. They have a smaller total budget and the same sized security staff as the small organization, but a larger need. They must rely on help from IT staff for plans and practices. Their ability to set policy, handle incidents, and effectively allocate resources is worse than any other size. However, they may be large enough to implement a multi-tiered approach to security, with fewer dedicated groups and more functions assigned to each group (Pages 12, 13).

11. **What are the purposes of security education, training, and awareness programs?** The purpose of Security Education, Training, and Awareness (SETA) programs is to enhance security by building in-depth knowledge, to design, implement, or operate security programs for organizations and systems. They develop skills and knowledge so that computer users can perform their jobs while using IT systems more securely and improve awareness of the need to protect system resources. They also aim to improve employee behavior, enable the organization to hold employees accountable for their actions, and inform members where to report (Pages 32, 33).

12. **How to make a SETA program effective?** To make a SETA program effective, a 7-step methodology generally applies:
    - Step 1: Identify program scope, goals, and objectives.
    - Step 2: Identify training staff.
    - Step 3: Identify target audiences.
    - Step 4: Motivate management and employees.
    - Step 5: Administer the program.
    - Step 6: Maintain the program.
    - Step 7: Evaluate the program (Page 46).

13. **What is access control?** Access controls regulate the admission of users into trusted areas of the organization. This includes both the logical access to the information systems and the physical access to the organization's facilities. Access controls are maintained by means of a collection of policies, programs to carry out those policies, and technologies that enforce policies. The applications of access controls include identification, authentication, authorization, and accountability (Page 5).

14. **What are the key principles of access control?** The key principles of access control include the principle of least privilege, which allows members of the organization to access the minimum amount of information for the minimum amount of time necessary to perform their required duties. The need-to-know principle limits a user's access to the specific information required to perform the currently assigned task, and not merely to the category of data required for a general work function. The separation of duties principle requires that significant tasks be split up in such a way that more than one individual is responsible for their completion (Page 6).

15. **What are the categories of access control?** The categories of access control include Preventative, Deterrent, Detective, Corrective, Recovery, and Compensating controls. These controls are depicted by their inherent characteristics. Another approach describes the degree of authority under which the controls are applied, including Mandatory Access Controls (MACs), Nondiscretionary Controls, and Discretionary Access Controls (DACs) (Pages 7, 10).

16. **What are the available access control techniques?** The document does not provide specific details about the access control techniques of "Something you know", "Something you have", "Something you are", and "Something you produce". However, these terms are typically associated with multi-factor authentication, a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.

17. **What is benchmarking and why do organizations do benchmarking?** Benchmarking is the process of following the existing practices of a similar organization or industry-developed standards. Organizations usually draw from established security models and practices to generate a security blueprint. Benchmarking can help to determine which controls should be considered but cannot determine how those controls should be implemented in your organization (Page 52).

18. **What are the categories of benchmarking? (due care/due diligence, recommended practices)** The categories of benchmarks include standards of due care/due diligence and best practices. Standards of due care/due diligence involve organizations adopting minimum levels of security for legal defense. They may need to show that they have done what any prudent organization would do in similar circumstances. Best practices include a sub-category of practices, called the gold standard, that are generally regarded as "the best of the best" (Page 53).

19. **What are the benefits and limitations of benchmarking?** The biggest barrier to benchmarking is that organizations don't talk to each other. A successful attack is viewed as an organizational failure and is kept secret, insofar as possible. However, more and more security administrators are joining professional associations and societies like ISSA and sharing their stories and lessons learned. An alternative to this direct dialogue is the publication of lessons learned (Page 58).

20. **What is baselining and why do organisations do baselining?** Baselining is a process of measuring against established standards. It provides a value or profile of a performance metric against which changes in the performance metric can be usefully compared (e.g., the number of attacks per week that an organization experiences). Baseline measurements of security activities and events are used to evaluate the organization's future security performance. Information gathered for an organization's first risk assessment becomes the baseline for future comparisons (Page 59).

21. **What is performance measurement and why do organisations do performance measurement?** Performance measurement is an ongoing, continuous improvement operation. Information security performance measures must be implemented and integrated into ongoing information security management operations. It is insufficient to simply collect these measures once. Costs, benefits, and performance of InfoSec are measurable, despite the claim of some CISOs that they are not. Measurement requires the design and ongoing use of an InfoSec performance management program based on effective performance metrics (Pages 63, 85).

22. **What is risk management?** Risk management is a process of identifying, examining, and understanding the threats facing the organization's information assets. It involves evaluating the risk controls, determining which control options are cost-effective, acquiring or installing the appropriate controls, overseeing processes to ensure that the controls remain effective, identifying risks, assessing risks, and summarizing the findings (Pages 3, 4, 6).

23. **How do organisations identify and assess risks?** Organizations identify and assess risks by first identifying the organization's information assets, classifying them into useful groups, and prioritizing them by their overall importance. They then identify and examine the threats facing these assets and assess the levels of risk in the organization. This includes asking questions such as which threats present a danger to the organization's assets

in the given environment, which threats represent the most danger to the organization's information, how much would it cost to recover from a successful attack, and which threats would require the greatest expenditure to prevent (Pages 5, 8, 32).

24. **Terms explained, e.g., information assets, threats, vulnerabilities, etc.**
    - Information Assets: These are the organization's data and information that need to be protected.
    - Threats: These are potential dangers to the organization's information assets.
    - Vulnerabilities: These are specific avenues that threat agents can exploit to attack an information asset (Pages 5, 8, 26).

25. **What are the results of risk assessment?** The results of risk assessment include a list of assets and their vulnerabilities, a ranked vulnerability risk worksheet, and a documentation package. The goals of the risk management process are to identify information assets and their vulnerabilities and to rank them according to the need for protection (Pages 45, 46, 49).

26. **What are the risk control strategies?** Risk control strategies involve evaluating the risk controls, determining which control options are cost-effective, acquiring or installing the appropriate controls, and overseeing processes to ensure that the controls remain effective. Three general categories of controls exist: Policies, Programs, and Technical controls (Pages 6, 42).

27. **Why do organisations do feasibility studies and what feasibility studies do they do?** The document does not provide specific details about why organizations do feasibility studies and what feasibility studies they do. However, in general, feasibility studies are conducted to evaluate the potential success of a proposed project or system. They may assess factors such as economic feasibility, technical feasibility, legal feasibility, operational feasibility, and scheduling feasibility.