1. Strategic planning	**2.** goals
3. objectives	**4.** strategic plan
5. tactical plans	**6.** Tactical planning
7. operational plans	**8.** corporate governance
9. operational planning	**10.** Governance

2. Sometimes used synonymously with *objectives*; the desired end of a planning cycle.	**1.** The process of defining and specifying the long-term direction (strategy) to be taken by an organization, and the allocation and acquisition of resources needed to pursue this effort.
4. The documented product of strategic planning; a plan for the organization's intended strategic efforts over the next several years.	**3.** Sometimes used synonymously with *goals*; the intermediate states obtained to achieve progress toward a goal or goals.
6. The actions taken by management to specify the intermediate goals and objectives of the organization in order to obtain specified strategic goals, followed by estimates and schedules for the allocation of resources necessary to achieve those goals and objectives.	**5.** The documented product of tactical planning; a plan for the organization's intended tactical efforts over the next few years.
8. Executive management's responsibility to provide strategic direction, ensure the accomplishment of objectives, oversee that risks are appropriately managed, and validate responsible resource use.	**7.** The documented product of operational planning; a plan for the organization's intended operational efforts on a day-to-day basis for the next several months.
10. "The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly."	**9.** The actions taken by management to specify the short-term goals and objectives of the organization in order to obtain specified tactical goals, followed by estimates and schedules for the allocation of resources necessary to achieve those goals and objectives.

11. de facto standards	**12.** Information security governance
13. Standards	**14.** de jure standards
15. information security policy	**16.** guidelines
17. practices	**18.** procedures
19. systems-specific security policies (SysSPs)	**20.** issue-specific security policy

12. The application of the principles of corporate governance to the information security function.	**11.** A standard that has been widely adopted or accepted by a public group rather than a formal standards organization. Contrast with a *de jure standard*.
14. A standard that has been formally evaluated, approved, and ratified by a formal standards organization. Contrast with a *de facto standard*.	**13.** A detailed statement of what must be done to comply with policy, sometimes viewed as the rules governing policy compliance. If the policy states that employees must “use strong passwords, frequently changed,” the standard might specify that the password “must be at least 8 characters, with at least one number, one
16. Nonmandatory recommendations the employee may use as a reference in complying with a policy. If the policy states to “use strong passwords, frequently changed,” the guidelines might advise that “we recommend you don’t use family or pet names, or parts of your Social Security number, employee number, or phone	**15.** Written instructions provided by management that inform employees and others in the workplace about proper behavior regarding the use of information and information assets.
18. Step-by-step instructions designed to assist employees in following policies, standards, and guidelines. If the policy states to “use strong passwords, frequently changed,” the procedure might advise that “in order to change your password, first click the Windows Start button, then….”	**17.** Examples of actions that illustrate compliance with policies. If the policy states to “use strong passwords, frequently changed,” the practices might advise that “according to X, most organizations require employees to change passwords at least semi-annually.”
20. An organizational policy that provides detailed, targeted guidance to instruct all members of the organization in the use of a resource, such as one of its processes or technologies.	**19.** Organizational policies that often function as standards or procedures to be used when configuring or maintaining systems. SysSPs can be separated into two general groups—managerial guidance and technical specifications—but may be written as a single unified SysSP document.

21. managerial guidance SysSPs	**22.** enterprise information security policy (EISP)
23. access control list (ACL)	**24.** access control matrix
25. capabilities table	**26.** technical specifications SysSPs
27. Configuration rules	**28.** policy administrator
29. sunset clause	**30.** Managerial controls

22. The high-level information security policy that sets the strategic direction, scope, and tone for all of an organization's security efforts. An EISP is also known as a security program policy, general security policy, IT security policy, high-level InfoSec policy, or simply an InfoSec policy.	**21.** A systems-specific security policy that expresses management's intent for the acquisition, implementation, configuration, and management of a particular technology, written from a business perspective.
24. An integration of access control lists (focusing on assets) and capability tables (focusing on users) that results in a matrix with organizational assets listed in the column headings and users listed in the row headings. The matrix contains ACLs in columns for a particular device or asset and capability tables in rows for a particular	**23.** Specifications of authorization that govern the rights and privileges of users to a particular information asset. ACLs include user access lists, matrices, and capabilities tables.
26. A type of systems-specific security policy that expresses technical details for the acquisition, implementation, configuration, and management of a particular technology, written from a technical perspective. Typically the policy includes details on configuration rules, systems policies, and access control.	**25.** A lattice-based access control with rows of attributes associated with a particular subject (such as a user).
28. An employee responsible for the creation, revision, distribution, and storage of a policy in an organization.	**27.** The instructions a system administrator codes into a server, networking device, or security device to specify how it operates.
30. Information security safeguards that focus on administrative planning, organizing, leading, and controlling, and that are designed by strategic planners and implemented by the organization's security administration. These safeguards include governance and risk management.	**29.** A component of policy or law that defines an expected end date for its applicability.

31. information security model	**32.** information security blueprint
33. information security framework	**34.** defense in depth
35. Operational controls	**36.** Technical controls
37. security perimeter	**38.** Redundancy
39. security education, training, and awareness (SETA)	**40.** security domains

32. In information security, a framework or security model customized to an organization, including implementation details.	**31.** See *information security framework*.
34. A strategy for the protection of information assets that uses multiple layers and different types of controls (managerial, operational, and technical) to provide optimal protection.	**33.** In information security, a specification of a model to be followed during the design, selection, and initial and ongoing implementation of all subsequent security controls, including information security policies, security education and training programs, and technological controls. Also known as a security model.
36. Information security safeguards that focus on the application of modern technologies, systems, and processes to protect information assets. These safeguards include firewalls, virtual private networks, and IDPSs.	**35.** Information security safeguards focusing on lower-level planning that deals with the functionality of the organization's security. These safeguards include disaster recovery and incident response planning.
38. The use of multiple types and instances of technology that prevent the failure of one system from compromising the security of information.	**37.** The boundary in the network within which an organization attempts to maintain security controls for securing information from threats from untrusted network areas. The advent of mobile and cloud information technologies makes the security perimeter increasingly difficult to define and secure.
40. An area of trust within which information assets share the same level of protection. Each trusted network within an organization is a security domain. Communication between security domains requires evaluation of communications traffic.	**39.** A managerial program designed to improve the security of information assets by providing targeted knowledge, skills, and guidance for an organization's employees.

41. adverse events	**42.** contingency planning (CP)
43. contingency plan	**44.** disaster recovery planning (DRP)
45. incident response planning (IRP)	**46.** business continuity planning (BCP)
47. incidents	**48.** disasters
49. incident response plan (IR plan)	**50.** business continuity plan (BC plan)

42. The actions taken by senior management to specify the organization's efforts and actions if an adverse event becomes an incident or disaster. This planning includes incident response, disaster recovery, and business continuity efforts, as well as preparatory business impact analysis.	**41.** An event with negative consequences that could threaten the organization's information assets or operations. Sometimes referred to as an incident candidate.
44. The actions taken by senior management to specify the organization's efforts in preparation for and recovery from a disaster.	**43.** The documented product of contingency planning; a plan that shows the organization's intended efforts in reaction to adverse events.
46. The actions taken by senior management to develop and implement the BC policy, plan, and continuity teams.	**45.** The actions taken by senior management to develop and implement the IR policy, plan, and computer security incident response team.
48. An adverse event that could threaten the viability of the entire organization. A disaster may either escalate from an incident or be initially classified as a disaster.	**47.** An adverse event that could result in loss of an information asset or assets, but does not currently threaten the viability of the entire organization.
50. The documented product of business continuity planning; a plan that shows the organization's intended efforts to continue critical functions when operations at the primary site are not feasible.	**49.** The documented product of incident response planning; a plan that shows the organization's intended efforts in the event of an incident.

51. business resumption planning, or BRP	**52.** disaster recovery plan (DR plan)
53. business impact analysis (BIA)	**54.** Maximum tolerable downtime (MTD)
55. Recovery time objective (RTO)	**56.** contingency planning management team (CPMT)
57. incident classification	**58.** Work recovery time (WRT)
59. Recovery point objective (RPO)	**60.** incident candidate

52. The documented product of disaster recovery planning; a plan that shows the organization's intended efforts in the event of a disaster.	**51.** The actions taken by senior management to develop and implement a combined DR and BC policy, plan, and set of recovery teams.
54. The total amount of time the system owner or authorizing official is willing to accept for a mission/business process outage or disruption, including all impact considerations.	**53.** An investigation and assessment of the various adverse events that can affect the organization, conducted as a preliminary phase of the contingency planning process, which includes a determination of how critical a system or set of information is to the organization's core processes and recovery priorities.
56. The group of senior managers and project members organized to conduct and lead all CP efforts.	**55.** The maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD.
58. The amount of effort (expressed as elapsed time) necessary to make the business function operational after the technology element is recovered (as identified with RTO). Tasks include testing and validation of the system.	**57.** The process of examining an incident candidate and determining whether it constitutes an actual incident.
60. See *adverse event*.	**59.** The point in time prior to a disruption or system outage to which mission/business process data can be recovered after an outage (given the most recent backup copy of the data).

61. alert roster	**62.** hierarchical roster
63. computer forensics	**64.** sequential roster
65. incident damage assessment	**66.** alert message
67. evidence	**68.** after-action review
69. full backup	**70.** incremental backup

62.
An alert roster in which the first person calls a few other people on the roster, who in turn call others. This method typically uses the organizational chart as a structure.

61.
A document that contains contact information for people to be notified in the event of an incident.

64.
An alert roster in which a single contact person calls each person on the roster.

63.
The process of collecting, analyzing, and preserving computer-related evidence.

66.
A scripted description of the incident that usually contains just enough information so that each person knows what portion of the IR plan to implement without slowing down the notification process.

65.
The rapid determination of how seriously a breach of confidentiality, integrity, and availability affected information and information assets during an incident or just following one.

68.
A detailed examination and discussion of the events that occurred, from first detection to final recovery.

67.
A physical object or documented information entered into a legal proceeding that proves an action occurred or identifies the intent of a perpetrator.

70.
The duplication of only the files that have been modified since the previous incremental backup.

69.
The duplication of all files for an entire system, including all applications, operating systems components, and data.

71. redundant array of independent disks (RAID)	**72.** disk striping
73. differential backup	**74.** disk mirroring
75. disk duplexing	**76.** hot swapped
77. warm site	**78.** server fault tolerance
79. hot site	**80.** service bureau

72. A RAID implementation (typically referred to as RAID Level 0) in which one logical volume is created by storing data across several available hard drives in segments called stripes.	**71.** A system of drives that stores information across multiple units to spread out data and minimize the impact of a single drive failure. By storing the data redundantly, the loss of a drive will not necessarily cause a loss of data. Also known as RAID.
74. A RAID implementation (typically referred to as RAID Level 1) in which the computer records all data to twin drives simultaneously, providing a backup if the primary drive fails.	**73.** The duplication of all files that have changed or been added since the last full backup.
76. A hard drive feature that allows individual drives to be replaced without powering down the entire system and without causing a fault during the replacement.	**75.** An approach to disk mirroring in which each drive has its own controller to provide additional redundancy.
78. A level of redundancy provided by mirroring entire servers to provide redundant capacity for services.	**77.** A facility that provides many of the same services and options as a hot site, but typically without installed and configured software applications. Warm sites are used for BC operations.
80. A continuity strategy in which an organization contracts with a service agency to provide a BC facility for a fee.	**79.** A fully configured computing facility that includes all services, communications links, and physical plant operations. Hot sites are used for BC operations.

81.
time-share

82.
cold site

83.
Remote journaling

84.
Mutual agreements

85.
Electronic vaulting

86.
database shadowing

87.
crisis management

82.
A facility that provides only rudimentary services, with no computer hardware or peripherals. Cold sites are used for BC operations.

81.
A continuity strategy in which an organization co-leases facilities with a business partner or sister organization. A time-share allows the organization to have a BC option while reducing its overall costs.

84.
A continuity strategy in which two organizations sign a contract to assist the other in a disaster by providing BC facilities, resources, and services until the organization in need can recover from the disaster.

83.
The backup of data to an off-site facility in close to real time based on transactions as they occur.

86.
A backup strategy to store duplicate online transaction data along with duplicate databases at the remote site on a redundant server. This server combines electronic vaulting with remote journaling by writing multiple copies of the database simultaneously to two locations.

85.
A backup method that uses bulk batch transfer of data to an off-site facility; this transfer is usually conducted via leased lines or secure Internet connections.

87.
An organization’s set of planning and preparation efforts for dealing with potential human injury, emotional trauma, or loss of life as a result of a disaster.