Define security control or safeguard.

Step 1:

A precaution or countermeasure recommended for an information system or organisation that is intended to ensure the privacy, accuracy, and availability of its data and to comply with a set of established security standards.

Security controls are safeguards or methods that reduce security risks to tangible assets such as information, computers, or other assets by preventing, detecting, countering, or minimising such hazards. These controls safeguard the availability, confidentiality, and integrity of information in the field of information security.

Step 2:

Examples include administrative controls like separation of roles, data classification, and auditing, as well as physical controls like fences, locks, and alarm systems, as well as technology controls like antivirus software, firewalls, and intrusion prevention systems.

Security measures play a fundamental part in determining the steps cyber security experts take to safeguard a firm.

Technical, administrative, and physical security controls are the three basic categories of IT security measures. A security control's main objective may be preventative, detective, corrective, compensating, or deterrent in nature. In the same way that regulations or training on social engineering are used to protect people, controls are also used to do so.

List and briefly define the three broad classes of controls and the three categories each can include.

Step 1:

Management control: Pay close attention to the security plans, standards, and policies that have an impact on the choice of operational and technical controls. Controls allude to problems that management must solve.

Operational: Take care of the proper application and utilisation of security policies.

Technical controls: Comprise the proper application of systems' hardware and software security features.

Step 2:

Management control: this includes policies, planning, guidelines, standards, and influencing the choice of additional protections.

- Operational: proper application and enforcement of policies, correction of operational flaws, carried out by individuals

- Technical controls: proper application of software and hardware security features

categories:

- Supportive controls: utilised in conjunction with numerous other controls, they offer some general security (identification, cryptographic key management)

- Preventive measures: guard against security lapses (authentication, access control)

- Controls for detection and recovery: find and report (attempted) breaches, aid in recovery (intrusion detection, audit)

 List a specific example of each of the three broad classes of controls from those given in Table 15.3.

Step 1:

Risk assessment, planning, system and service acquisition, and security evaluations are all examples of management controls.

Security of personnel, physical protection, emergency planning, upkeep, incident response, awareness, and training are operational controls

Technical controls: System and Communications Protection, Access Control, Audit, Identification and Authentication,