1. Các nhóm kiểm soát

Trong an toàn thông tin, các biện pháp kiểm soát (**controls**) được chia thành ba nhóm chính:

- **Kiểm soát hành chính/Quản lý (Administrative/Managerial controls)**
- **Kiểm soát kỹ thuật (Technical controls)**
- **Kiểm soát vật lý/Vận hành (Physical/Operational controls)**

1.1 Kiểm soát hành chính/Quản lý

Nhóm này xử lý yếu tố con người trong an toàn thông tin. Bao gồm chính sách và quy trình quy định cách tổ chức quản lý dữ liệu, cũng như trách nhiệm của nhân viên trong việc bảo vệ tổ chức.
Mặc dù chủ yếu dựa trên chính sách, nhưng việc thực thi có thể cần sử dụng thêm kiểm soát kỹ thuật hoặc vật lý.

1.2 Kiểm soát kỹ thuật

Bao gồm các giải pháp như **firewall, intrusion detection systems (IDS), intrusion prevention systems (IPS), antivirus (AV), encryption**... Các kiểm soát này giúp tổ chức đạt được mục tiêu bảo mật.

1.3 Kiểm soát vật lý/Vận hành

Bao gồm khóa cửa, khóa tủ, camera giám sát, thiết bị quẹt thẻ,... nhằm hạn chế quyền truy cập vật lý vào tài sản khỏi những người không có thẩm quyền.

2. Các loại kiểm soát

Các loại kiểm soát bao gồm (nhưng không giới hạn):

- **Ngăn chặn (Preventative)**
- **Khắc phục (Corrective)**
- **Phát hiện (Detective)**
- **Răn đe (Deterrent)**

Các kiểm soát này kết hợp với nhau tạo thành **defense in depth** để bảo vệ tài sản.

- **Preventative**: ngăn chặn sự cố xảy ra ngay từ đầu.
- **Corrective**: khôi phục sau sự cố.
- **Detective**: phát hiện sự cố đang xảy ra hoặc đã xảy ra.
- **Deterrent**: răn đe, làm nản lòng kẻ tấn công.

2.1 Administrative/Managerial Controls

Control Name	Control Type	Control Purpose
Least Privilege	Ngăn chặn	Giảm rủi ro và tác động từ insider hoặc tài khoản bị chiếm đoạt
Disaster recovery plans	Khắc phục	Đảm bảo tính liên tục trong kinh doanh
Password policies	Ngăn chặn	Giảm khả năng bị brute force hoặc dictionary attack
Access control policies	Ngăn chặn	Tăng cường tính bảo mật bằng cách quy định nhóm được truy cập/chỉnh sửa dữ liệu
Account management policies	Ngăn chặn	Quản lý vòng đời tài khoản, giảm bề mặt tấn công, hạn chế nguy cơ từ nhân viên cũ hoặc tài khoản mặc định
Separation of duties	Preventative	Giảm rủi ro và tác động từ insider hoặc tài khoản bị chiếm đoạt

2.2 Kiểm soát kỹ thuật

Tên kiểm soát	Loại kiểm soát	**Mục đích**
Firewall	Ngăn chăn	Lọc bỏ traffic độc hại hoặc không mo
IDS/IPS	Phát hiện	Phát hiện và ngăn chặn traffic bất thường khớp với signature/rule
Encryption	Răn đe	Bảo mật thông tin nhạy cảm

Backups	Khắc phụctive	Khôi phục dữ liệu sau sự cố
Password management	Ngăn chặn	Giảm tình trạng mệt mỏi mật khẩu
Antivirus (AV) software	Ngăn chặn	Quét, phát hiện và cách ly mối đe dọ
Manual monitoring, maintenance, and intervention	Ngăn chặn	Quản lý mối đe dọa, rủi ro từ hệ thống lỗi thời

2.3 Kiểm soát vật lý/Vận hành

Tên kiểm soát	**Loại kiểm soát**	**Mục đích**
Time-controlled safe	Răn đe	Giảm nguy cơ từ đe dọa vật lý
Adequate lighting	Răn đe	Hạn chế nơi ẩn nấp, giảm nguy cơ tấ
Closed-circuit television (CCTV)	Ngăn chặn/phát hiện	Ngăn ngừa sự cố và hỗ trợ điều tra sa
Locking cabinets (for network gear)	Ngăn chặn	Ngăn truy cập trái phép vào thiết bị r
Signage indicating alarm service provider	Răn đe	Giảm khả năng tấn công thành công
Locks	Răn đe/ngăn chặn	Ngăn truy cập trái phép vào tài sản
Fire detection and prevention (fire alarm, sprinkler system, etc.)	Phát hiện/ Ngăn chặn	Phát hiện cháy và giảm thiệt hại tài sản