Access Control Practices

* Deny access to systems to undefined users or anonymous accounts.
* Limit and monitor the usage of administrator and other powerful accounts.
* Suspend or delay access capability after a specific number of unsuccessful logon attempts
* Remove obsolete user accounts as soon as the user leaves the company
* Suspend inactive accounts after 30 to 60 days.
* Enforce strict access criteria.
* Enforce the need-to-know and least-privilege practices. （least privilege : giving an employee the only enough rights and privilege to carry out what they are supposed to do and nothing more)
* Disable unneeded system features, services and ports.
* Replace default password settings on accounts.
* Limit and monitor global access rules.
* Remove redundant resource rules from accounts and group memberships.
* Remove redundant user IDs, accounts, and role-based accounts from resource access lists.
* Enforce password rotation.
* Enforce password requirements (length, contents, lifetime, distribution, storage, and transmission).
* Audit system and user events and actions, and review reports periodically.
* Protect audit logs.

Security controls

* Safeguards to prevent, detect, correct or minimise security risks.
* Set of actions for data security

**Definition**

Security Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks.

**Advantages**

* A principle benefit of the Controls is that they prioritize and focus a smaller number of actions with high pay-off results.
* The Controls are effective because they are derived from the most common attack patterns highlighted in the leading threat reports and vetted across a very broad community of government and industry practitioners.

What is it for?

* They were created to answer the question, "what do we need to do to stop known attacks."
* The key to the continued value is that the Controls are updated based on new attacks that are identified and analysed by groups from Verizon to Symantec so the Controls can stop or mitigate those attacks.

**There are Two ways of categorising Security Controls:**

1. Categorising according to nature of the control

* Administrative Controls
* Technical Controls/ Logical Controls
* Physical Controls

2. Categorising according to the different phases of the control process

* Deterrent
* Preventative
* Detective
* Corrective
* Recovery/ Compensatory

Categorising according to nature of the control

1. **Administrative Controls**

These include the developing and publishing of policies, standards, procedures, and guidelines; risk management; the screening of personnel; conducting security-awareness training; and implementing change control procedures.

Definition

* Administrative controls refer to policies, procedures, or guidelines that define personnel or business practices in accordance with the organisation's security goals.
* Administrative controls are the process of developing and ensuring compliance with policy and procedures.
* They tend to be things that employees may do, or must always do, or cannot do.

Categories of Administrative Controls:

* Policies
* Standards
* Procedures
* Guidelines

Examples:

* Policies(Eg. Business Continuity Plan, Access Control Policy, Disaster Recovery Plan）
* Procedures
* Personnel Controls ( Def: Personnel controlling indicates strengths and weaknesses of the company. Its purpose is to effectively exploit the potential of all employees to achieve the maximum benefit within the organisation.）
* Supervisory structure (Def: a board of management of which nonmanagerial workers are members, having supervisory powers over some aspects of management decision-making.)
* Testing ( Eg. Vulnerability Scanning, Penetration Testing, Security Audit/Review, Risk Assessment, Security Scanning)

1. **Technical Controls (aka Logical Controls)**

These consist of implementing and maintaining access control mechanisms, password and resource management, identification and authentication methods, security devices, and the configuration of the infrastructure.

Definition:

Technical controls are the hardware and software components that protect a system against cyberattacks. Firewalls, intrusion detection systems (IDS), encryption, and identification and authentication mechanisms are examples of technical controls.

May refer to：

* identification and authentication methods
* security devices
* configuration of the infrastructure

Examples：

Preventative

* Encryption
* Smart cards
* Network authentication
* Access control lists (ACLs)
* File integrity auditing software
* patching
* IPS

Detective

* Security logs
* NIDS
* HIDS

Corrective/Recovery

* IPS
* Restore from backups
* patching

1. **Physical Controls**

Depending on the organization physical security countermeasures will vary. A government agency such as the Department of Defense may have armed guards at the door of the building. Many organizations are not in the position of breaching national security so armed guards are not a necessity. In many cases a receptionist greets any new visitors and makes the appropriate arrangements for an on-site visit.

Definition:

These entail controlling individual access into the facility and different departments, locking systems and removing unnecessary floppy or CD-ROM drives, protecting the perimeter of the facility, monitoring for intrusion, and environmental controls.

Examples:

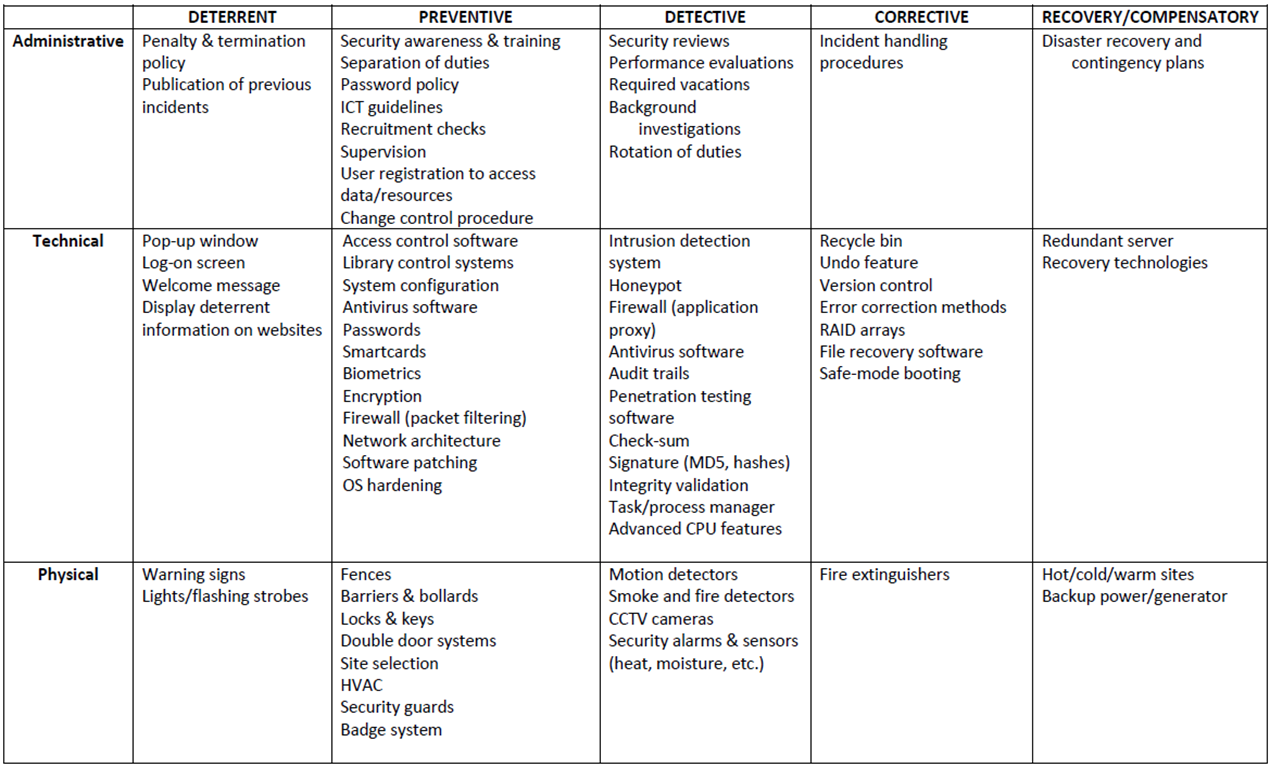
* Automated barriers & bollards
* Building management systems like Heating, HVAC, lifts/elevators control, etc.
* CCTV- Closed Circuit TV
* Electronic article surveillance - EAS
* Fire detection
* GIS mapping systems
* Intercom & IP phone
* Lighting control system
* Perimeter intrusion detection system
* Radar based detection & Perimeter surveillance radar
* Security alarm
* Video wall
* Power monitoring system
* Laptop Locks

Categorising according to the different phases of the control process

* Deterrent: controls to discourage attacks at the first place, deter people from breaching security, e.g warning, banner, logon message, fake CCTV cameras to warn people, security measures on websites to tell people that they are protected
* Preventive: controls that make it hard for attacks to succeed, e.g. firewall (stops unwelcomed traffic), encryption, locked doors
* Detective: controls that detect if an attack has occurred, e.g. checksum, intrusion detection system, rotation of duties, security audits, monitors and sensors, motion sensors installed in the buildings to detect intruders, CCTV cameras, sometimes firewall that tells when an attack has been made on the system, intrusion detection systems that monitor the activity on the hosts and computers over the network
* Corrective: corrective aspects of security, controls that reverse the damage, e.g. version control, incident handling procedures, fire extinguishers, undo, recycle bin, DOS attack (ban the IP addresses to stop from jamming the servers), Fire extinguishers (putting out fires when it has happened), Incident handling procedures (tells employees what to do when an incident happens)
* Recovery: controls that bring the system back after a major disaster like earthquakes or tsunamis , e.g. disaster recovery plan, hot/cold/warm sites, backup power,

A general example:

Speeding (have fines and punishment, and preventive controls like speed bumps, detection – security cameras)



Categorising according to the different phases of the control process

1. **Deterrent:** controls to discourage attacks at the first place, deter people from breaching security, e.g warning, banner, logon message, fake CCTV cameras to warn people, security measures on websites to tell people that they are protected
2. **Preventive:** controls that make it hard for attacks to succeed, e.g. firewall (stops unwelcomed traffic), encryption, locked doors
3. **Detective:** controls that detect if an attack has occurred, e.g. checksum, intrusion detection system, rotation of duties, security audits, monitors and sensors, motion sensors installed in the buildings to detect intruders, CCTV cameras, sometimes firewall that tells when an attack has been made on the system, intrusion detection systems that monitor the activity on the hosts and computers over the network
4. **Corrective:** corrective aspects of security, controls that reverse the damage, e.g. version control, incident handling procedures, fire extinguishers, undo, recycle bin, DOS attack (ban the IP addresses to stop from jamming the servers), Fire extinguishers (putting out fires when it has happened), Incident handling procedures (tells employees what to do when an incident happens)
5. **Recovery:** controls that bring the system back after a major disaster like earthquakes or tsunamis , e.g. disaster recovery plan, hot/cold/warm sites, backup power,

Real-life Example

**Speeding:** deterrent - having fines and punishment, preventive controls like speed bumps, detection security cameras, corrective - enforcement of fines and punishments, recovery -

**Fire Hazards:** *deterrent* - flyers or advertisements how to prevent fire hazards from happening, *preventive* - making sure no open stoves are left unattended, power sockets are turned off when not in use, *detective* - smoke detectors, cctv at home, *corrective -* fire extinguishers, *recovery -* insurance and funds kept for a rainy day

**Commonly Used Security Methods**

To address the key requirements of the AIC triad, one can employ a number of commonly used security methods:

* Least privilege
* Defense-in-depth
* Minimization
* Keep things simple
* Compartmentalization
* Use choke points
* Fail securely/safely
* Leverage unpredictability
* Separation of duties

**Least Privilege**

**States that:** do not provide more privileges than are required. This applies to both users and applications.

* Example: No administrative rights to guests accounts, unidentified applications should not be able to have the power to change the system file etc.)
* This principle applies not only to privileges of users and applications on a computer system, but also to other noninformation systems privileges of an organization’s staff.
* The principle of least privilege is a preventive control, because it reduces the number of privileges that may be potentially abused and therefore limits the potential damage.
* Some examples of application of this principle include the following:
* Giving users only read access to shared files if that’s what they need, and making sure write access is disabled
* Not allowing help desk staff to create or delete user accounts if all that they may have to do is to reset a password
* Not allowing software developers to move software from development servers to production servers
* Privilege : The ability to access data to run processes and applications
* Product: keep system more stable by giving less privilege to untrustworthy users

**Advantages:**

* Minimizes the attack surface, diminishing avenues a malicious actor can use to access sensitive data or carry out an attack by protecting superuser and administrator privileges.
* Reduces malware propagation by not allowing users to install unauthorized applications. The principle of least privilege also stops lateral network movement that can launch an attack against other connected devices by limiting malware to the entry point.
* Improves operational performance with reductions in system downtime that might otherwise occur as a result of a breach, malware spread or incompatibility issues between applications.
* Safeguards against human error that can happen through mistake, malice or negligence.

**Disadvantages:**

The two big problems with least privilege are minimal access and expiration of access.

* Minimal access

When assigning or providing access, in many cases an admin is not sure whether or not someone needs access. In the past, if an admin was not sure if a user needed access, the default rule was to go ahead and provide the user with access. While this potentially minimized support desk calls and user frustration, it introduced considerable risk.

If you provide additional access and it is not needed, no one ever notifies the help desk. Ultimately, providing access to a user beyond what he or she needs to perform his/her role leads to a massively increased attack surface that leaves organizations wide open to damage from hackers and insiders.

* Expiration of access

The second big problem with data access is expiration. In most organizations, once access is provided to a piece of information, it is never removed.Over the course of employment at an organization, as a user’s role and responsibilities change (or the technologies they need to access grow), more access is granted to the user. However, rarely is the previous access, when no longer relevant to a user’s role, removed.

**Importance:**

* The principle of least privilege is an important information security construct for organizations operating in today’s hybrid workplace to help protect them from cyberattacks and the financial, data and reputational losses that follow when ransomware, malware and other malicious threats impact their operations.
* The principle of least privilege strikes a balance between usability and security to safeguard critical data and systems by minimizing the attack surface, limiting cyberattacks, enhancing operational performance and reducing the impact of human error.

**Defense in Depth** (multiple types of security controls in different layers)

* The principle of defense in depth is about having more than one layer or type of defense.
* **Advantage**: The reasoning behind this principle is that any one layer or type of defense may be breached, no matter how strong and reliable you think it is, but two or more layers are much more difficult to breach.
* **Disadvantages:** It is usually more costly and time consuming to implement many layers of security.
* Defense in depth works best when you combine two or more different types of defense mechanisms—
* such as using a firewall between the Internet and your LAN, plus the IP Security Architecture (IPSEC) to encrypt all sensitive traffic on the LAN. In this scenario, even if your firewall is compromised, the attackers still have to break IP Security to get to your data flowing across the LAN.

Eg.

1st layer – Deterrent control (easy to implement, use it to warn hackers to not attack, breaching policies may not be legal)

2nd layer – Preventive control (Firewall installed on server that monitors all the traffic gg btw the internet and internal network and intercept any suspicious activities)

3rd layer – Detective layer (Network monitoring tools like intrusion detection systems that will alert ppl on any attacks being made on the system)

4th layer – Corrective layer (software installed like antivirus that could get rid of virus that the computer has been infected)

5th layer – Recovery layer (Data backup, another image of the system software for recovery in the event that the system breaks)

Generally, different types of controls should be used together:

* first, preventive controls should be in place to try and prevent security incidents from happening at all;
* second, detective controls are necessary so that you can know whether preventive controls are working or have failed;
* and third, corrective controls are needed to help you respond effectively to security incidents and contain damage.
* However, the defense in depth principle does not mean that you should indiscriminately apply all the controls and security measures you can get your hands on: balance has to be found between security provided by the defense in depth approach and the financial, human, and organizational resources you are willing to expend following it. This balance is addressed by the cost-benefit analysis.

**Minimisation**

***Purpose/Definition/Principle/****States that:*  the system should not run any applications that are not strictly required to complete its assigned task

* The minimization principle is the cousin of the least privilege principle and mostly applies to system configuration.
* For **example**, a computer whose only function is to serve as an e-mail server should have only e-mail server software installed and enabled. All other services and protocols should either be disabled or not installed at all to eliminate any possibility of compromise or misuse.
* **Advantages/Importance**:
* Adherence to the minimization principle not only increases security but usually also improves performance, saves storage space, and is a good system administration practice in general.
* Minimisation is also one of the cheapest methods as no additional costs are needed and it can help an organisation save cost on storage as well.
* Data minimization can help you reduce data theft by decreasing your data footprint that requires security. The principle also allows you to limit the number of records that may be affected in case of a data breach, thereby protecting your business against costly fines.

**Keep Things Simple**

Definition/ Principle： a security system should be kept simple as any complexity introduced leads to insecurity in the overall system

* Complexity is the worst enemy of security. Complex systems are inherently more insecure because they are difficult to design, implement, test, and secure.
* The more complex a system, the less assurance we may have that it will function as expected.
* Although complexity of information systems and processes is bound to increase with our increasing expectations of functionality, we should be very careful to draw a line between avoidable and unavoidable complexity and not sacrifice security for bells and whistles, only to regret it later.
* When you have to choose between a complex system that does much and a simple system that does a bit less but enough, choose the simple one.

**Compartmentalisation**

to prevent the compromise of the entire system, use a compartment approach to the system design and implementation

* Compartmentalization, or the use of compartments (also known as zones, jails, sandboxes, and virtual areas), is a principle that limits the damage and protects other compartments when software in one compartment is malfunctioning or compromised.
* Real life example: It can be best compared to compartments on ships and submarines, where a disaster in one compartment does not necessarily mean that the entire ship or submarine is lost.
* **Definition**: Compartmentalization in the information security context means that applications run in different compartments are isolated from each other. In such a setup, the compromise of web server software, for example, does not take down or affect e-mail server software running on the same system but in a separate compartment.
* **Advantages/Importance:** In information security, compartmentalization is equally about spreading the risk so if there’s any impact (breach) we’ve limited the damage to our personal information and the harm and recovery effort are far less.

**Use Choke Points**

**Purpose:** the traffic can be easier to analyse and control by using choke points

Security is very much about control, and control is so much more effective and efficient when you know all ways in and out of your systems or networks.

**Definition:** Choke points are logical “narrow channels” that can be easily monitored and controlled.

**Example:** An example of a choke point is a firewall—unless traffic can travel only via the firewall, the firewall’s utility is reduced to zero. Consider the example of controlled entrances to buildings or facilities of high importance, such as perimeter fencing and guard posts.

**Importance:** Enforcing choke points increases efficiency.

Attackers typically must go through a series of steps to steal assets. They will often breach defenses, move laterally, escalate privileges, evade detection, then exfiltrate data.

Mapping and prioritizing the choke points that attackers move though when launching attacks is a key approach for ensuring that critical assets stay safe. This strategy can also solve resource constraints — an important advantage for perennially understaffed/under-provisioned IT departments.

**Advantages:** The greatest advantage of the Choke-Point architecture is its single point of installation. This provides simple installation and reduced IT management. In the case of a Web Proxy Server, access performance may be enhanced due to the caching nature of the proxy.

**Disadvantages:** There are, however, a number of disadvantages to this architecture. The benefits of having a single point of installation also create a potential single point of failure that must be addressed with redundancy. Since the web filtering and reporting functionality in a Choke-Point environment requires all Web access to occur through a single point, the workstations in the managed environment must be configured to direct Web access to the Choke-Point. It is therefore possible for a user to change their configuration or use alternate means to access the Web. This could include a readily available WiFi connection or a portable Internet access device. In addition, monitoring and filtering remote or mobile users that are not in the managed environment requires the remote workstations to be directed back into the Choke-Point – a highly inefficient means to manage traffic.

**Conclusion from advantages and disadvantages:** Although somewhat offset by its caching capabilities, Choke-Point installations create a bottleneck to Internet content which, depending on traffic dynamics, may actually cause performance to suffer. In general, with respect to filtering, Choke-Point architectures are used primarily for Web content and typically do not address other Internet communication protocols such as content exposed in email, chat, IM and dark web postings.

Not cost effective as one would need to hire people and funds might be needed to install Choke-points.

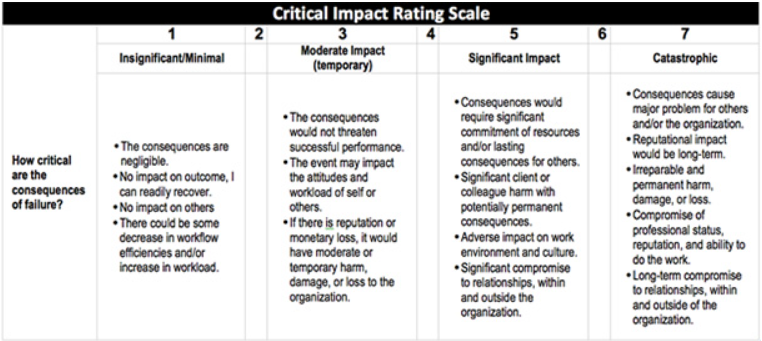
**Fail Securely**

**Definition:** Failing securely means that if a security measure or control has failed for whatever reason, the system is not rendered to an insecure state.

**Principle:** Whenever access, privileges, or some security-related attribute is not explicitly granted, it should be denied.

**Example:** For example, when a firewall fails, it should default to a “deny all” rule, not a “permit all.” However, fail securely does not mean “close everything” in all cases; if we are talking about a computer-controlled building access control system, for example, in case of a fire the system should default to “open doors” if humans are trapped in the building. In this case, human life takes priority over the risk of unauthorized access, which may be dealt with using some other form of control that does not endanger the lives of people during emergency situations.

**Advantages/Importance:** Fail securely is especially important for systems that are accessible to everyone as the traffic flow of such systems would be high, leading to an increase in probability of error or malicious attacks. Failing securely gives operators more time to figure out what went wrong and prevent any undetectable damage.



**Disadvantage:** Fail securely should not be used for systems where the impact of failure is significant or catastrophic. The consequences of failure, no matter how secure, could cause other major and significant damage such as reputational impact or adverse impact on work environment and culture for some organisations. Thus an organisation should weigh their impacts on the consequences of failure before using the Fail Securely method.

May not be the most expensive option, but is not cheap either because of the cost of such software and human resources to detect errors whenever fail securely happens.

**Secure the Weakest Link**

Many information security principles and approaches may sound like little more than common sense. Although that may well be the case, it doesn’t help us much, because very often we still fail to act with common sense.

**Definition/Principle:** Securing the weakest means to spend your security budget securing the biggest problems and the largest vulnerabilities.

**Advantages/Importance:** Instead of securing the weakest link, whatever it may be, resources are spent on reinforcing already adequate defences. The weakest link is the one most likely to be compromised by a hacker. An organisation's security model should not fall apart just because a part of the business, or a business partner, has weak security. Therefore securing the weakest link is important to decrease the chances of hackers exploiting the flaws of an organisation.

**Examples:** For example, there are technological solutions already employed to protect the system but no training on how to handle attachments in email messages. Securing the weakest link is the training of employees to handle attachment in email messages.

**Real life examples:** Addressing the weakest link means you avoid a strategy similar to erecting a gate and expecting an attacker to run straight for it while there are no walls around the gate to limit their access. With a focus on the weakest link, you expend your time and energy on the risks that matter most.

**Disadvantages:** Should be paired with other methods as well as may not work as well alone.

**Leverage Unpredictability**

**Definition/Principle:** Do not provide any information about the system's security setup - users and clients can know that a system is in place but they do not need any specific details

**Example:** Don’t publicise the specifics of their armaments, exact locations, or numbers of armed forces, you should not publicize the details of your security measures and defenses.

**FYI:**This principle should not be seen as contradicting deterrent security controls—controls that basically notify everyone that security mechanisms are in place and that violations will be resisted, detected, and acted upon. The important difference here is that deterrent controls don’t provide details of the defenses but merely announce their existence so as to deter potential attackers without giving them detailed information that later may be used against the defenders.

**Examples:** In practical terms, this means you can, for example, announce that you are using a firewall that, in particular, logs all traffic to and from your network, and these logs are reviewed by the organisation—there is no need to disclose the type, vendor, or version number of the firewall; where it is located; how often logs are reviewed; and whether any backup firewalls or network intrusion detection systems are in place.

**Importance:** Providing excessive information about a system’s security set up can lead to key information being lost or stolen, create a poor experience for customers and reputational harm.

**Segregation of Duties**

**Purpose/Definition:**  Segregation of duties can prevent or discourage security violations and should be practised when possible.

**Principle:** Although the actual job titles and organizational hierarchies may differ greatly, the idea behind the principle of separation of duties stays the same: no single person should be able to violate security and get away with it. Rotation of duties is a similar control that is intended to detect abuse of privileges or fraud and is a practice to help your organization avoid becoming overly dependent on a single member of the staff. By rotating staff, the organization has more chances of discovering violations or fraud.

**Most Cost Effective Method**

"Keep things simple" would be the one that would be the cheapest and easiest to implement as its aim is to have less complex solutions and reduce attack surface area and potential vulnerabilities. This can be achieved by reducing the number of components, protocols and systems in a network and reducing the amount of customization. Having a simple design makes it easier to secure, monitor, and maintain.