## CIA Triad

* **Confidentiality**: Assurance that data objects, resources and processes are not accessible to unauthorized subjects
* **Integrity**: 3 goals

1. Unauthorized subjects should not be able to make changes.
2. Authorized subjects should not be able to make unauthorized changes
3. Objects should remain internally and externally consistent, i.e. a given input produces the expected output. e.g. [Referential integrity](http://en.wikipedia.org/wiki/Referential_integrity), which involves prevention of errors in [Foreign Key](http://en.wikipedia.org/wiki/Foreign_Key) to [Primary Key](http://en.wikipedia.org/wiki/Primary_key) relationships, such as an orphan child record that is missing its parent record (sometimes termed a dangling foreign key).

* **Availability**: Authorized subjects are granted timely and uninterrupted access to objects
* Opposite of CIA is DAD: disclosure, alteration and destruction
* A computer system is **vulnerable** to virus attacks if the virus definitions in its anti-virus software are outdated. There is a **threat** of a virus attacking the system because it is exposed to a potentially harmful infection. The probability of a virus causing damage is considered a **risk**. Updating the virus definitions for the anti-virus software is a **countermeasure** that will mitigate the risk.
* Countermeasures mitigate risks, not vulnerabilities.

### Other Security Issues

* Privacy
* Authentication
* Authorization
* Access Control
* Data Validation
* Accountability

## Data Classification

**Government data classification (US DoD)**

* Unclassified – data not sensitive or classified
* Sensitive but Unclassified – minor secret, if disclosed can cause serious damage (e.g. medical data)
* Confidential
* Secret – if disclosed can cause serious damage to national security
* Top Secret – if disclosed can cause grave damage to national security

**Commercial classification schemes** are descriptive, eg

* Confidential – data exempt from freedom of information act, internal use only, disclosure can adversely affect company
* Private – personal information for use in the company, disclosure can adversely affect personnel
* Sensitive – higher assurance of integrity is required
* Public – disclosure not welcome, but not harmful (low impact)
* Other classifications may be
  + Proprietary – disclosure could reduce competitive edge
  + Based on asset value, usefulness lifespan, regulatory requirements

Principle of least privilege

* Authorized subjects are granted the minimum amount of privileges (for the minimum amount of time) required to complete their task.

Separation of duties

* One person cannot complete a task on their own
* Two man controls - two people pushing two buttons at the same time to launch bomb, no one can reach both buttons
* Split knowledge: two or more people are required to open a bank safe, not one knows the whole combination.

## Hiring and Firing Employees

**Termination Procedures**

* Exit interview
  + Surrender keys, badges, etc.
  + Remove employee form work environment
  + Remind employee of employment and non-disclosure agreements
* (meanwhile…) Employee’s network user accounts are disabled
* Security escort to collect personal belongings
* Make sure employee returns company property from vehicle or home

## Security Roles

* Senior Manager or organization owner, must sign off on all policy issues, responsible for exercising due care and due diligence in establishing security. Decision makers.
* Security Professional, InfoSec officer or CIRT, responsible for following directives of senior manager, Has the functional responsibility for security, writes the security policy and implements.
* Data Owner, High level manager responsible for safeguarding the data he or she is assigned: assign classification level, access control policy, maintain inventory and accounting
* Data Custodian, responsible *day-to-day security administration*: data backup and restore, directory and file permissions, assigning (revoking) users to groups, implements the prescribed protection defined by security policy, data management tasks
* User, any person with access to secure system
* Auditor, test and verify security policy is implemented, role may be assigned to a security professional or a trained user.

## Security Roles

## Security Management Planning

1. Strategic plan, a long-term fairly stable plan. Organizations’ goals, mission and objectives; also a risk assessment
2. Tactical plan, ~1 year. Eg: project plans, acquisition plans, hiring plans, buget plans, maintenance plans, support plans and system development plans.
3. Operational plan, short term, highly detailed. Updated often (quarterly or monthly)

## Policies, standards, baselines, guidelines and procedures

An effective information security policy should

* be designed with a **long-term focus**.
* include separation of duties
* be understandable and supported by all stakeholders
* specify areas of authority and responsibility

### Security Policies

1. Organizational security policy
2. Issue-specific security policy
3. System-specific security policy
4. Regulatory – industry or legal standards apply
5. Advisory – defines “acceptable” and consequences of violations
6. Informative – provide knowledge, eg goals, mission statement

### Formalized Security Policy Structure

* 1. Policies
  2. Standards
  3. Baselines
  4. Guidelines
  5. Procedures

## Risk Management

The elements of risk

1. Assets, which are endangered by
2. Threats, exploit
3. Vulnerabilities, which result in
4. Exposure, which is
5. Risk, which is mitigated by
6. Safeguards, which protect… Assets

### Quantitative Risk Analysis

|  |  |  |
| --- | --- | --- |
| 1 | AV – asset value | inventory assets and assign a value |
| 2 | EF – exposure factor, %  SLE = AV \* EF | research each asset, list possible threats, calculate the EF and SLE |
| 3 | ARO = # / year | threat analysis to calc likelihood of each threat in a single year |
| 4 | ALE = SLE \* ARO = AV \* EF \* ARO | overall loss potential per threat |
| 5 | ACS = $ / year | research cost of countermeasures |
| 6 | Value or benefit of a safeguard  [ALE1 – ALE2] – ACS | cost / benefit analysis of each countermeasure for each threat for each asset |

**qualitative impact analysis**

* Advantage: it prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities.
* Disadvantage: does not provide specific quantifiable measurements of the magnitude of the impacts, therefore making a cost-analysis of any recommended controls difficult.
* Since it involves a lot of guesswork, it can not be easily automated.

### Three Commonly Recognized Learning Levels

* + Awareness
  + Training
  + Education