Domain 1:
Security and Risk Management

- 1.5 Understand, adhere to, and promote professional ethics
  - (ISC)² Code of Professional Ethics
  - Organizational code of ethics

- 1.6 Develop, document, and implement security policy, standards, procedures, and guidelines

Domain 1:
Security and Risk Management

- 1.7 Identify, analyze, and prioritize Business Continuity (BC) requirements
    - ➢ Develop and document scope and plan
    - ➢ Business Impact Analysis (BIA)

- 1.8 Contribute to and enforce personnel security policies and procedures
    - ➢ Candidate screening and hiring
    - ➢ Employment agreements and policies
    - ➢ Onboarding and termination processes
    - ➢ Vendor, consultant, and contractor agreements and controls
    - ➢ Compliance policy requirements
    - ➢ Privacy policy requirements

Domain 1:
Security and Risk Management

- 1.9 Understand and apply risk management concepts
  - ➢ Identify threats and vulnerabilities
  - ➢ Risk assessment/analysis
  - ➢ Risk response
  - ➢ Countermeasure selection and implementation
  - ➢ Applicable types of controls (e.g., preventive, detective, corrective)
  - ➢ Security Control Assessment (SCA)
  - ➢ Monitoring and measurement
  - ➢ Asset valuation
  - ➢ Reporting
  - ➢ Continuous improvement
  - ➢ Risk frameworks

Domain 1:
Security and Risk Management

- 1.10 Understand and apply threat modeling concepts and methodologies
    - ➢ Threat modeling methodologies
    - ➢ Threat modeling concepts

- 1.11 Apply risk-based management concepts to the supply chain
    - ➢ Risks associated with hardware, software, and services
    - ➢ Third-party assessment and monitoring
    - ➢ Minimum security requirements
    - ➢ Service-level requirements

Domain 1:
Security and Risk Management

- 1.12 Establish and maintain a security awareness, education, and training program
    - Methods and techniques to present awareness and training
    - Periodic content reviews
    - Program effectiveness evaluation

Key buzz words

- Organization means an entity or a company where you work. It can be private, public or a multi national.
- Authorize means you have access.
- Availability means it is available to you when you need it.
- All the material is agnostic which means that you can apply the concepts in any organization or industry as applicable per their business, security and compliance requirements.

What is CIA and the difference between them

1.1 Understand and apply concepts of confidentiality, integrity and availability

The CIA Connection

The CIA connection:

CIA means Confidentiality, Integrity, Availability

Confidentiality:

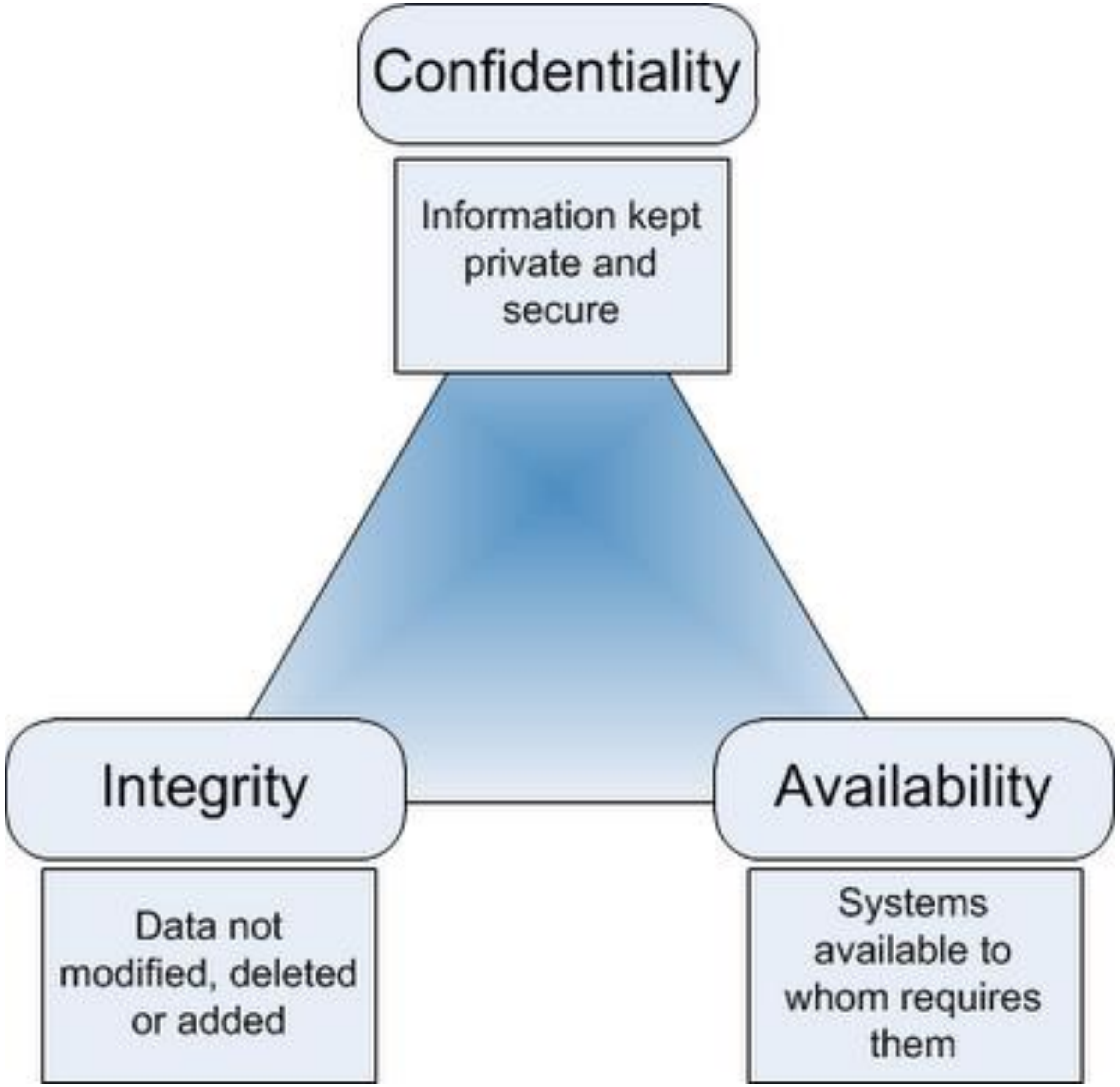
Only those who are authorizes to have access to the data can access the data.

Integrity:

Only those who are authorizes to make changes can modify the data

Availability:

Only those who are authorizes to access data can do so when permitted.



Confidentiality

Information kept private and secure

Integrity

Data not modified, deleted or added

Availability

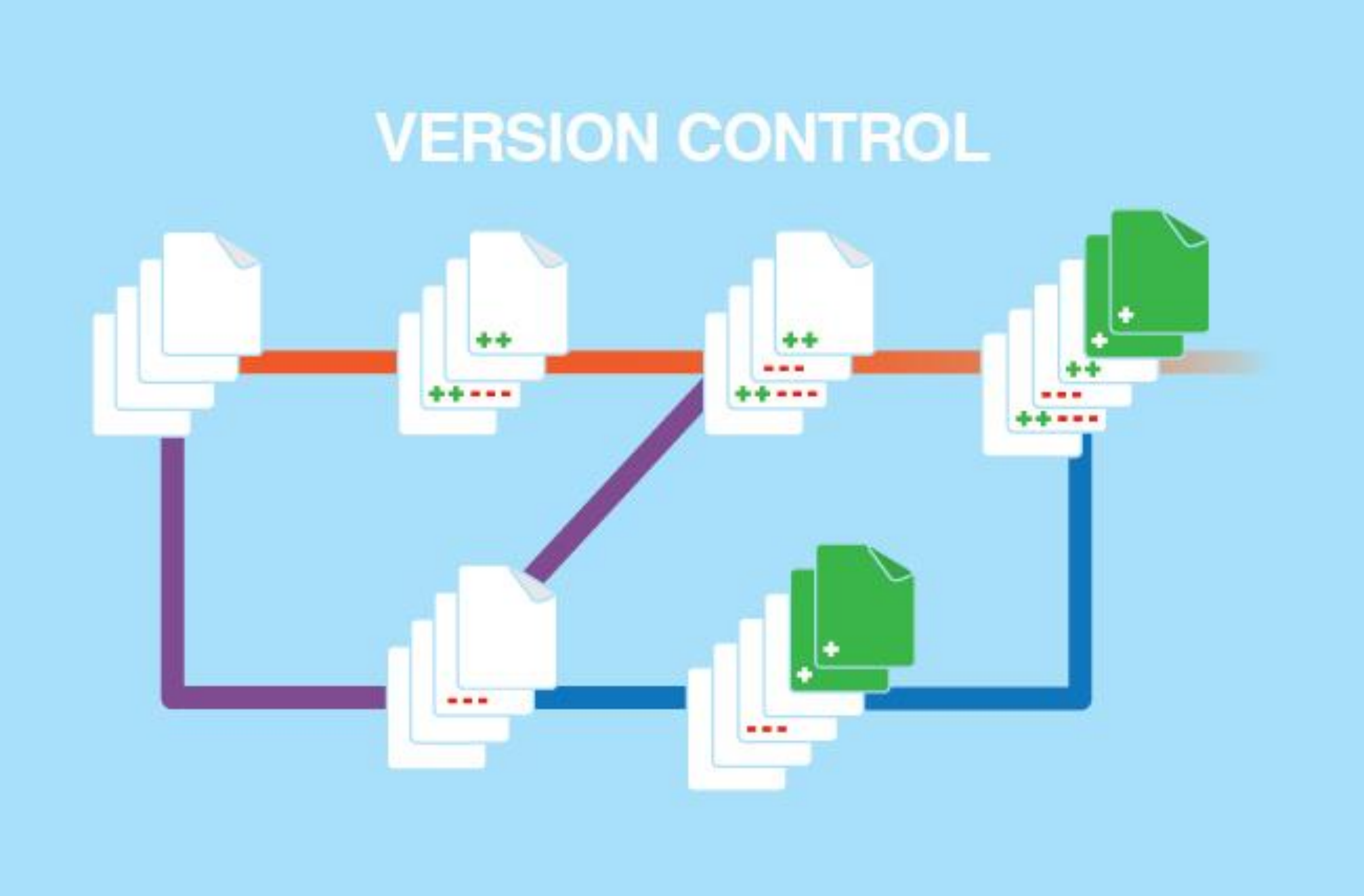
Systems available to whom requires them

Reference http://geraintw.blogspot.com/2012/09/cia-infosec.html

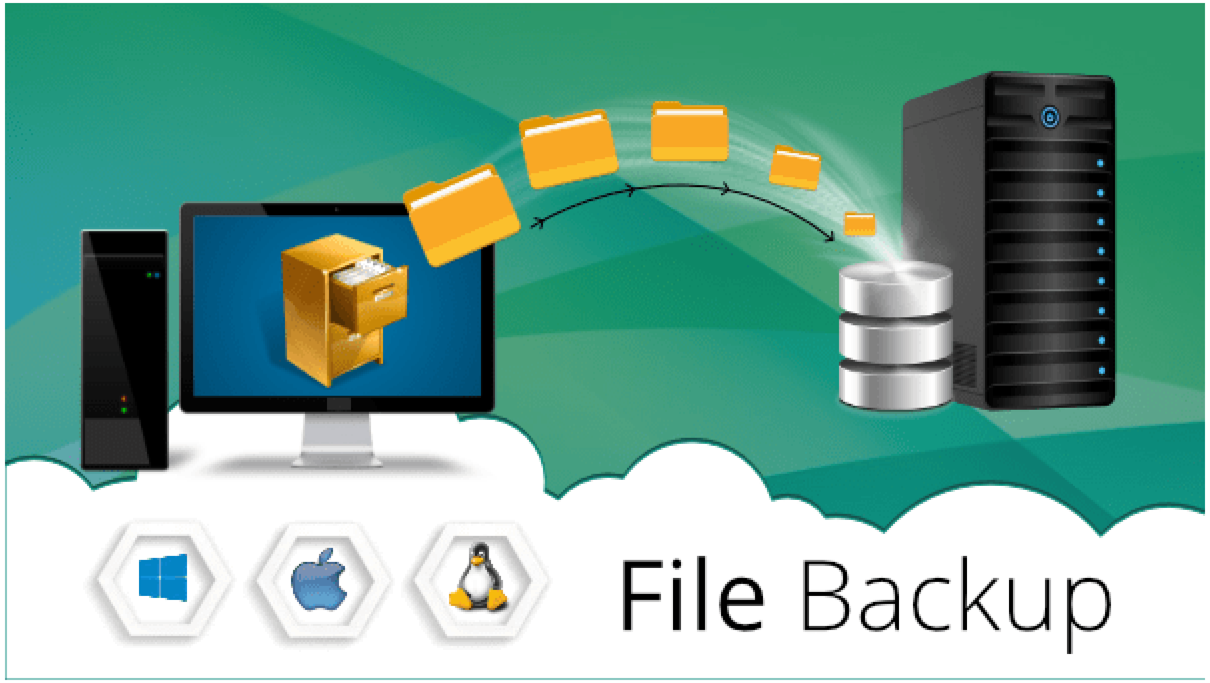
Confidentiality examples

© 2018 Al-Nafi. All Rights Reserved.

Integrity example

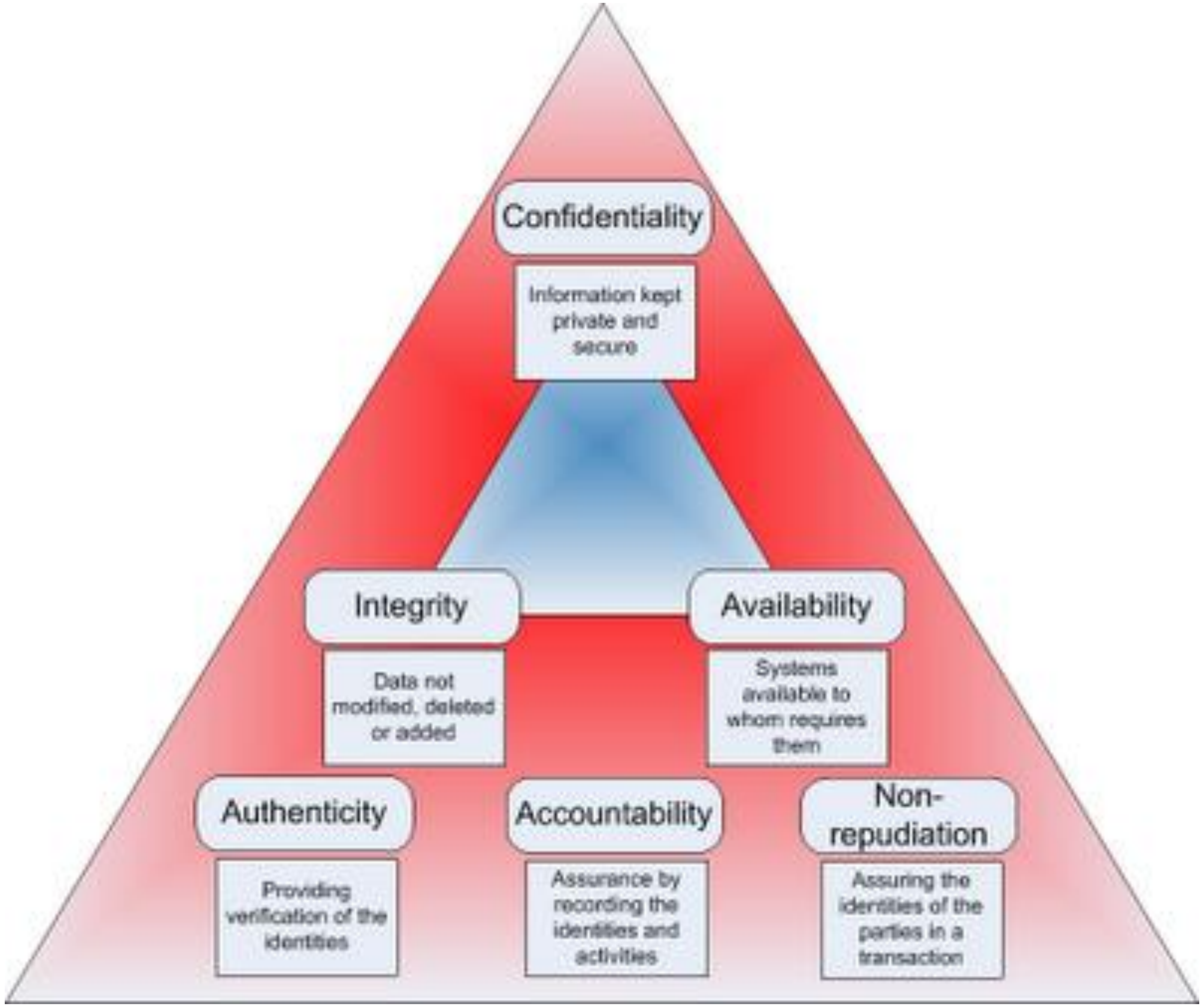


Availability examples



Additional CIA properties

- Authenticity on authentication - verification of the identity
- Accountability - assurance of a transaction by providing audit ability
- Non-repudiation - assurance of the transaction by validity of the transaction



Confidentiality

Information kept private and secure

Integrity

Data not modified, deleted or added

Availability

Systems available to whom requires them

Authenticity

Providing verification of the identities

Accountability

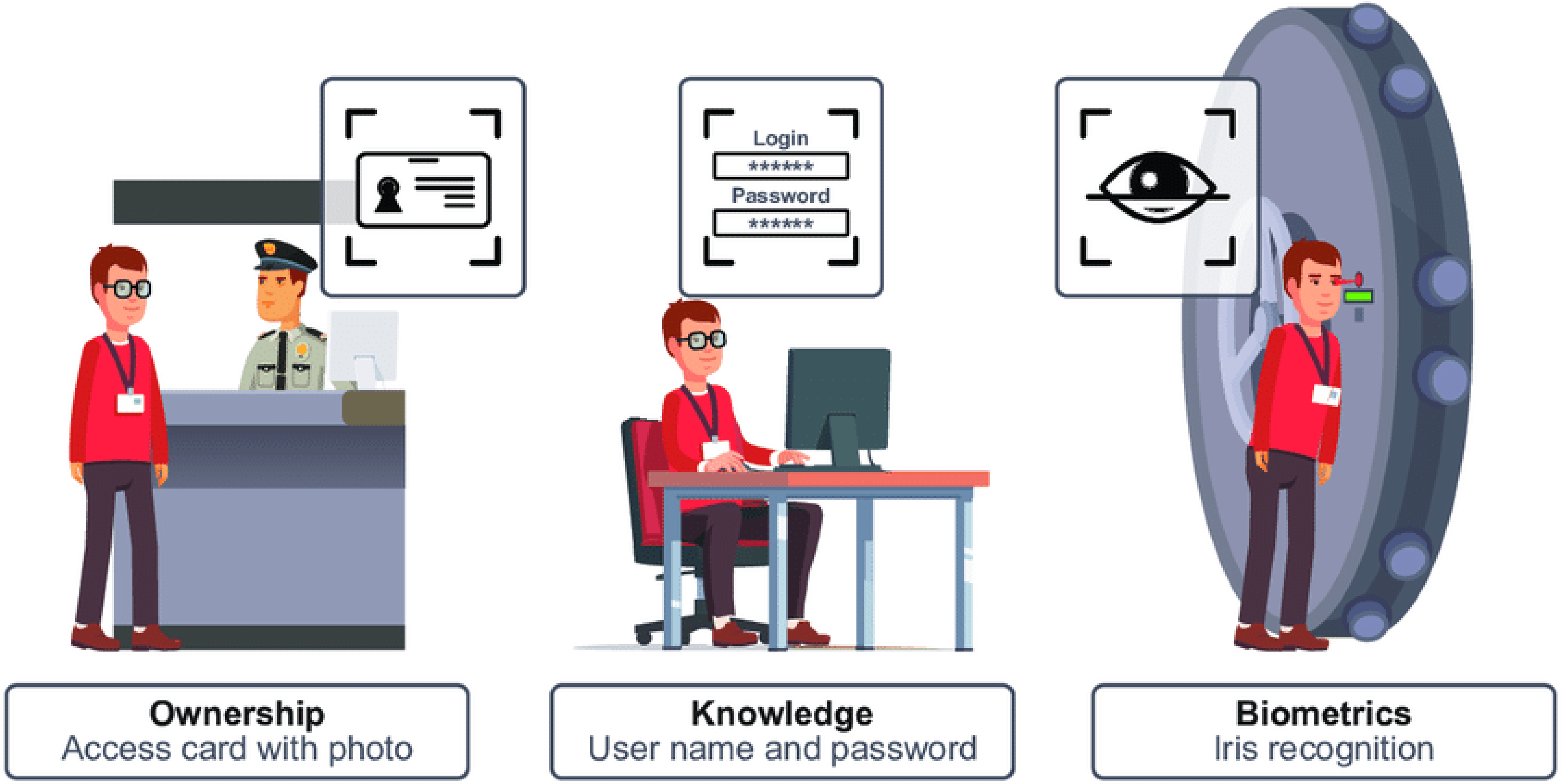
Assurance by recording the identities and activities

Non-repudiation

Assuring the identities of the parties in a transaction

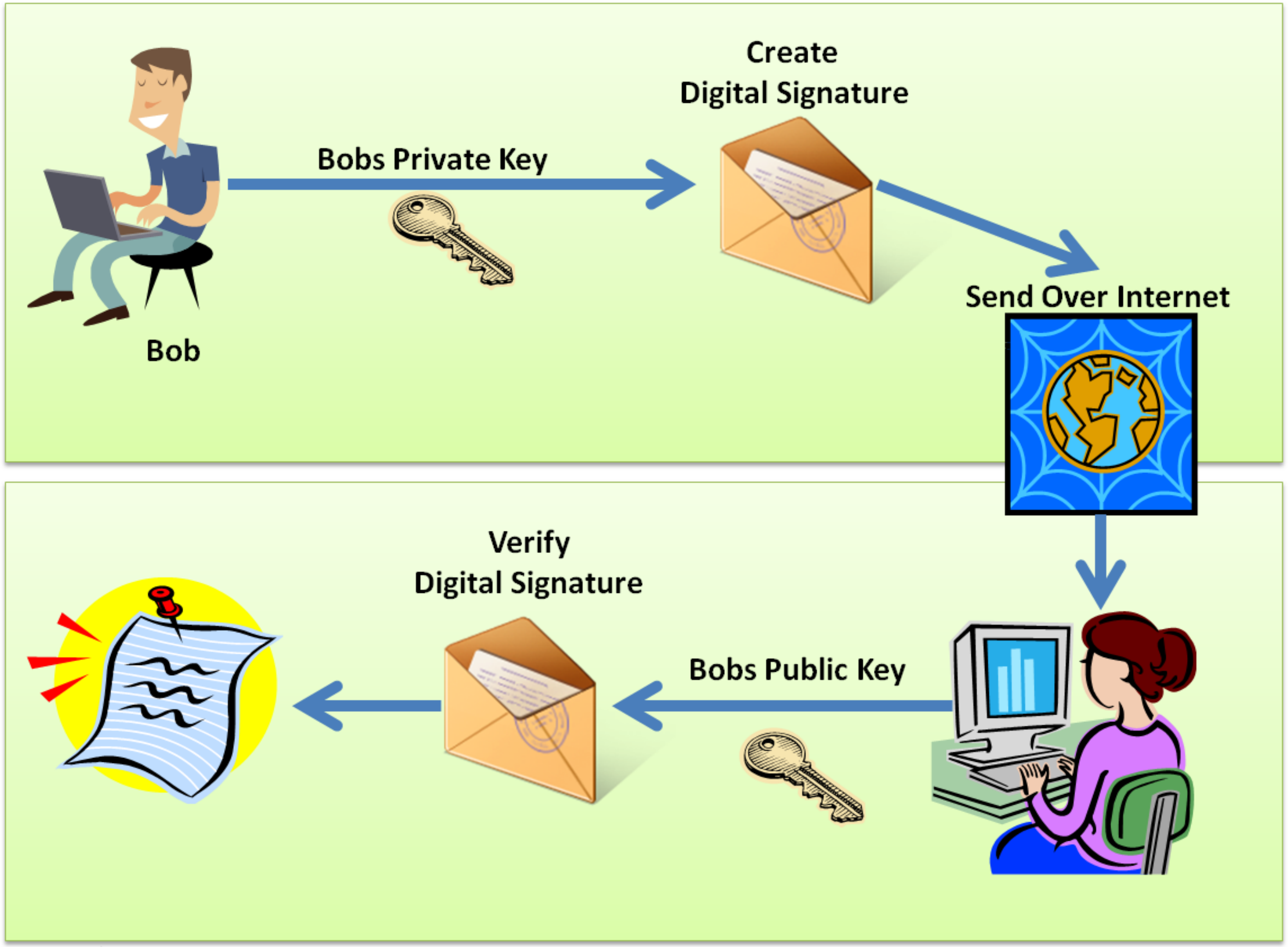
Reference http://geraintw.blogspot.com/2012/09/cia-infosec.html

Authenticity or Authentication examples!



Nonrepudiation examples

- Signing a contract.
- Making a credit card purchase at the store
- Audit logs in computer systems etc.
- Digital signatures



Security & Corporate Governance

- 1.2 Evaluate and apply security governance principles
    - ➢ Alignment of security function to business strategy, goals, mission, and objectives
    - ➢ Organizational processes (e.g., acquisitions, divestitures, governance committees)
    - ➢ Organizational roles and responsibilities
    - ➢ Security control frameworks
    - ➢ Due care/due diligence