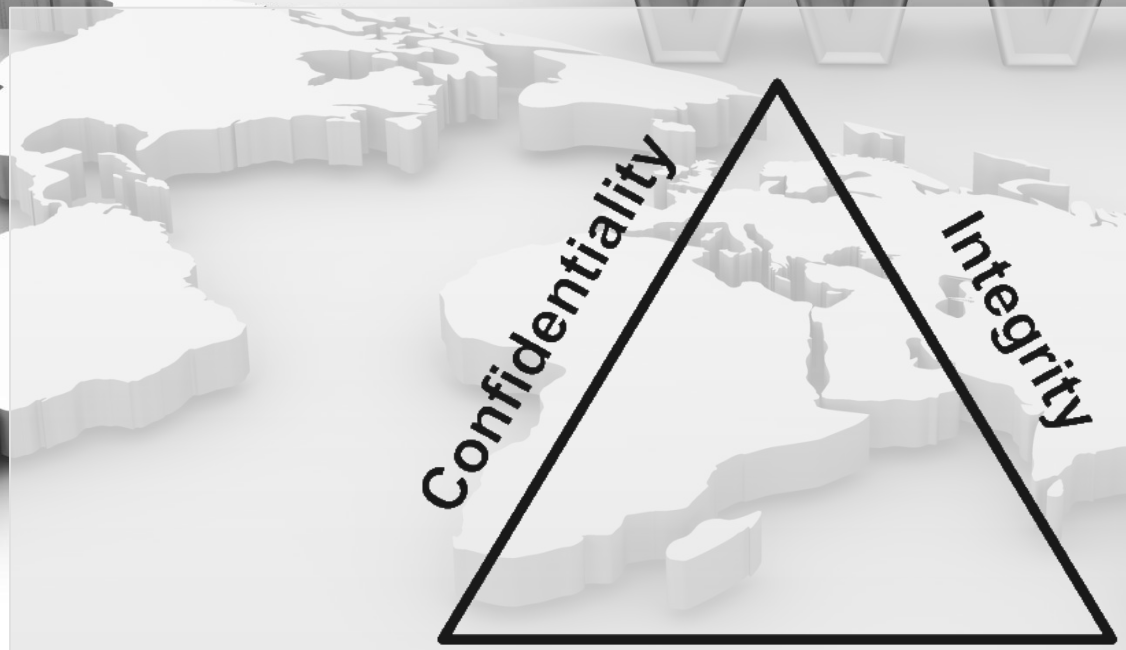
Azeemkhan.net

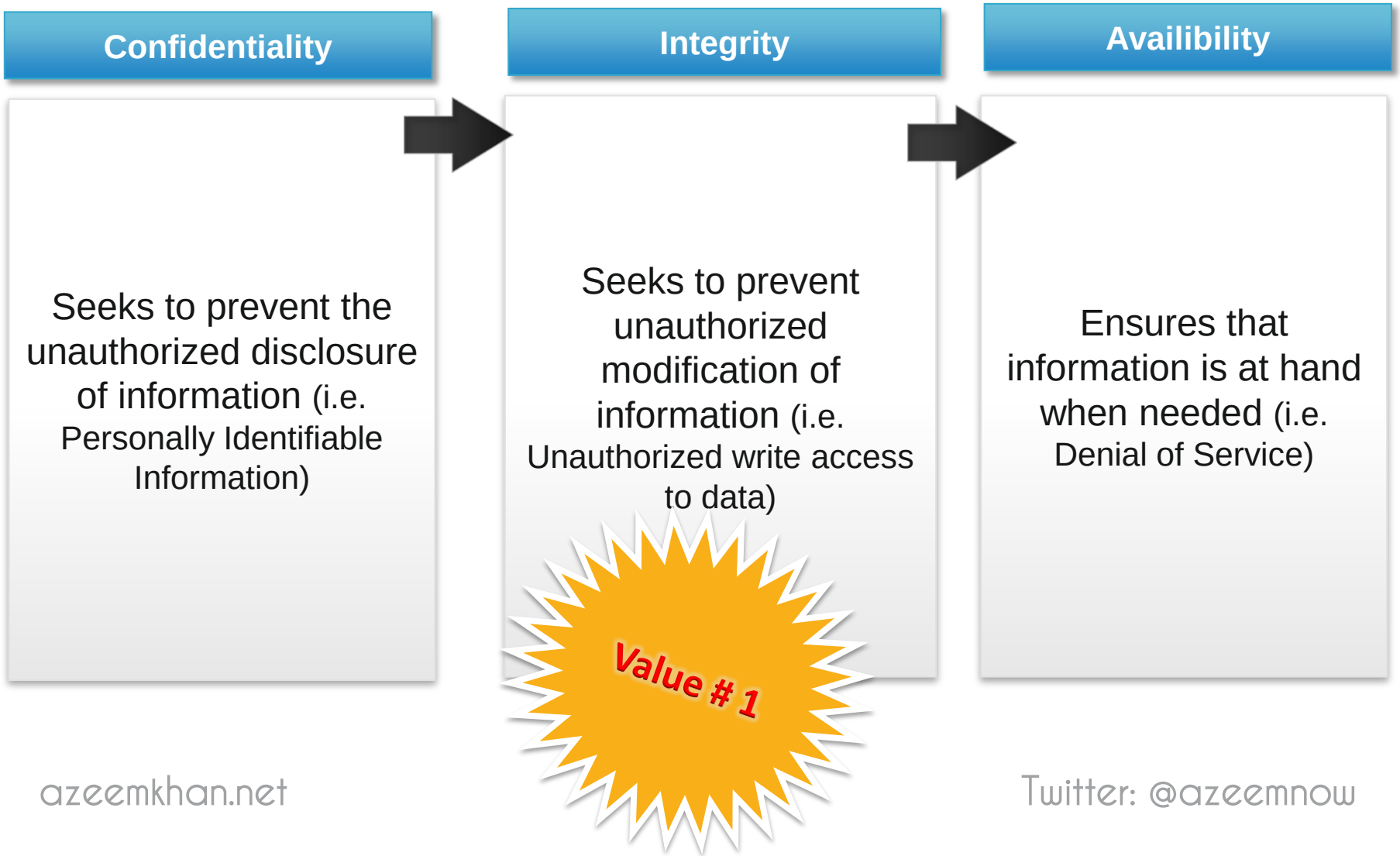
CISSP - 10 Domains : 15 Key Value Points

2013

Security Foundation



Cryptography



Cryptography – CIA: Confidentiality

Symmetric / Private	Asymmetric / Public
Same key to encrypt & decrypt message	Two keys: one public & one private
One key is shared between two or more entities	One entity has a public key, and the other entity has a private key
Algorithm is less complex and faster	Algorithm is more complex and slower
Incompatible with Digital Signatures	Enables Digital Signatures
Ex: Des, AES, 3DES,	Ex: ECC, DH, RSA

Cryptography – CIA: Integrity

Value # 3

- We can encrypt data so that it is private; but how do we know it has not been tampered with?
- **HASH Functions:** SHA-1, MD5
  - Variable length plaintext is “hashed” into a fixed-length hash value (message digest)
  - Referred to as “one way” because there is not way to reverse the hash algorithm

Hash alogirthm applied to a message → Results in a Message Digest → MD value is signed with sender’s Private Key → Produces Digital Signature

Cryptography in Use

- Link Level
  - Headers and all payload is encrypted
  - Decryption at each hop – if node is compromised, all traffic going through that node can be compromised
- End-to-End
  - Only payload is encrypted; headers is in plain
  - Hops do not need to decrypt headers

Access Control

I - AAA

IDENTITY & AUTHENTICATION

- Identity is a claim; without proof
- Proving an identity claim is Authentication:
  - Something you have, Something you know, Something you are

AUTHORIZATION

Actions you can perform on a system once you have been identified & authenticated: i.e. Read, Write, Read/Write

ACCOUNTING

- Holding users accountable for their actions via logging and analyzing audit data.
- Non-repudiation
  - Cannot deny having performed a transaction

Access Control Model

DAC, MAC, RBAC

Discretionary

1

- Data owner decides who can access resources
- Data owner is usually the creator & has full control of object
- Implemented through ACL's
- Used in environments that do not require a high level of centralized security

Mandatory

2

- Access is based on security clearance of subject and classification of object
- Each user is assigned a clearance, and each object has a classification
- Access is decided by the system policy and not up to the discreation of a data owner

Role-Based

3

- Allows access to objects based on the role the user holds within the company
- Administrators assign a user to a role & then assign access rights to that role, not directly to the user.
- Ideal for high rate of turnover

Architecture & Design

Security Models

Bell-LaPadula

- Divides entities into subjects and objects
- Clearance of the subject attempting to access an object is compared with that object's classification
- Confidentialtiy model

Biba

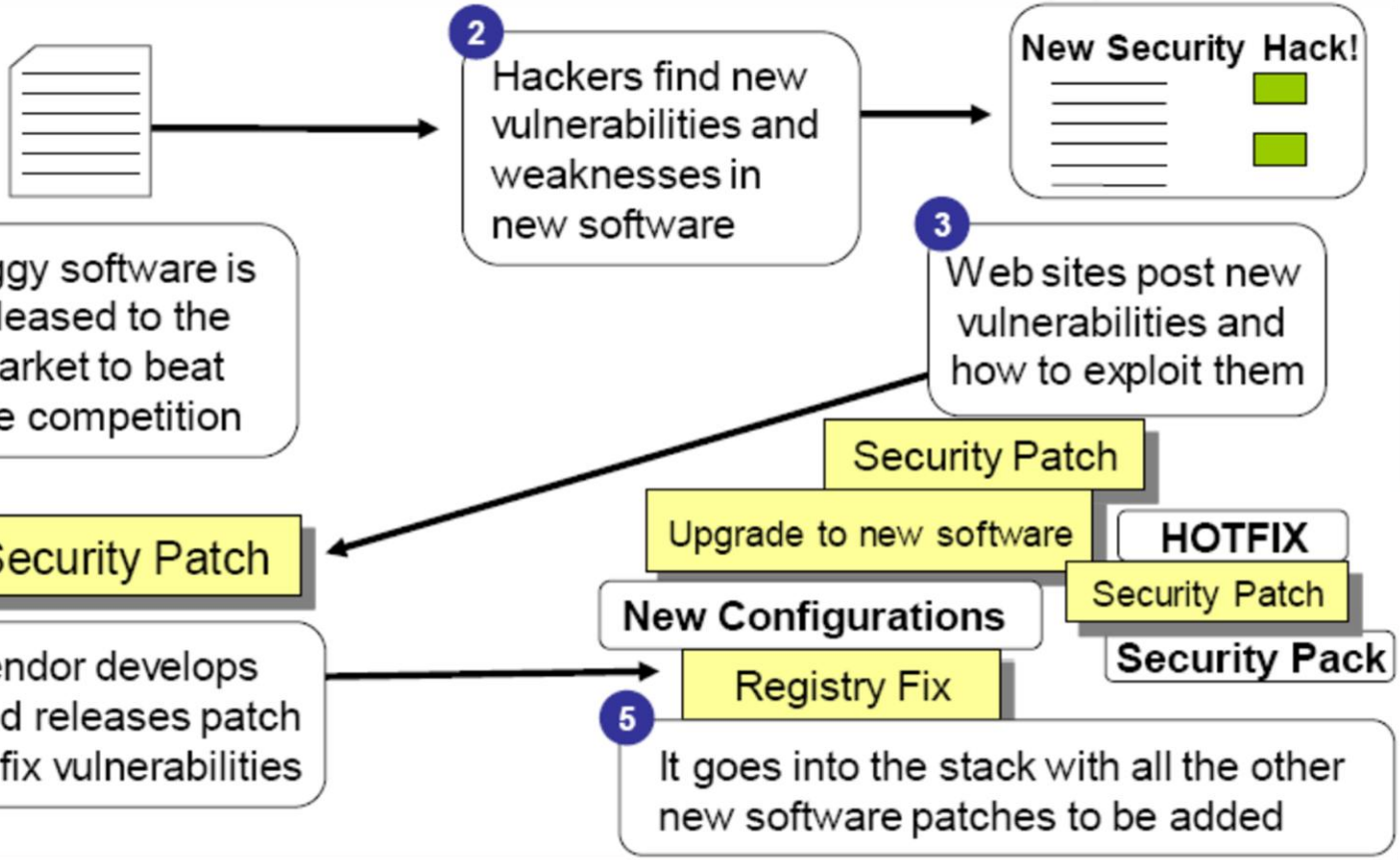
- Integrity model
- Subject cannot write data to an object at a higher integrity level
- Subjects cannot read data from an object at a lower integrity level

Clark-Wilson

- Separtion of duties: ensures consistency of data
- Prevents users from making improper modification
- Subject must go through a program to access & modify data

Software Development
Common Process for Address Flaws

Value #8



Telecommunication

Intrusion Detection System

Value # 9

Attack Detection

- Able to alert if you are under attack, or if a system on your network is compromised

Policy Enforcement

- Monitors network behavior that violates your organization's network security or acceptable use policies (i.e. social media, IM)

Audit Trial

- An IDS can provide an after-the-attack audit trail for seeking how far an attacker got, and where it came from

Resource Justification

- IDS can provide info on how well your firewall is working & how many people are "out to get you"

Telecommunication

Firewalls

Packet Filtering: 1st Gen

- Simplest, least expensive
- Based on addresses, ports, protocol type
- Cannot keep state info

Proxy: 2nd Gen

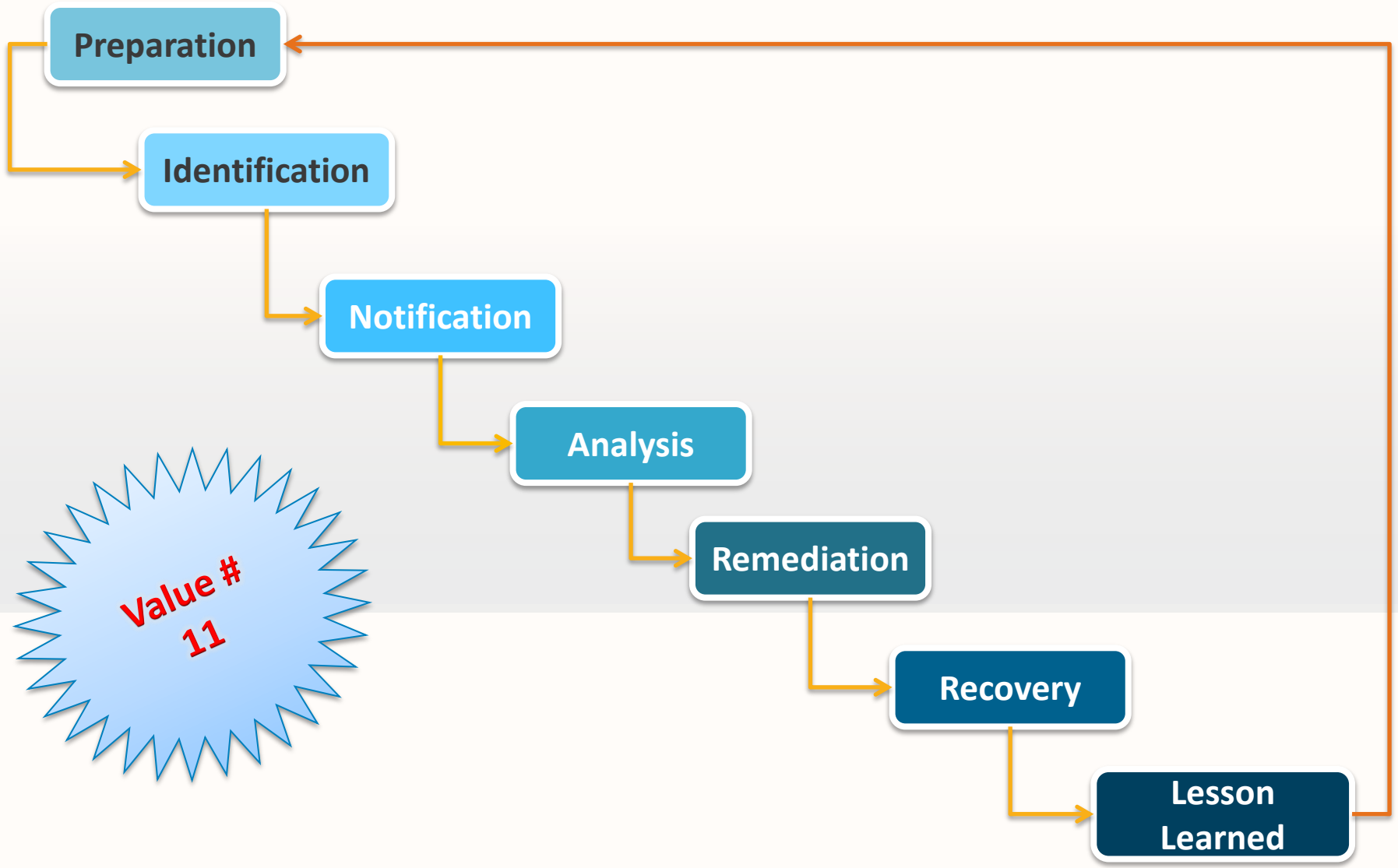
- Makes copy of each packet & transfers it from one network to another
- No direct connection between inside/outside
- Inserts its own address
- Application-level: deep packet inspection

Stateful: 3rd Gen

- Packets are captured by inspection engine & each OSI layer of the packet is inspected
- Keeps track of “state” communication stream; state table

Telecommunication

Life Cycle Of An Incident



Legal

Liabilities – who is at fault?

Due Care – doing the right thing

Performing ongoing maintenance necessary to keep something in proper working order
Opposite: negligence

Due Diligence - Investigation

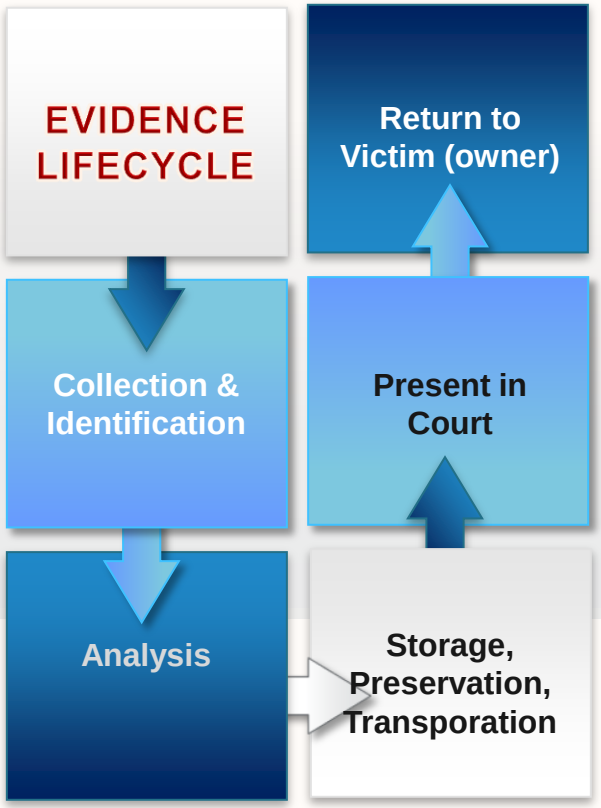
Performing research before committing to a course of action
Opposite: haphazardly; not doing your homework

- Did management fail to execute Due Care and/or Due Diligence?
- **Prudent Man Rule**:
  -Perform duties that prudent people (highest integrity) would exercise in similar circumstances
- **Downstream Liabilities**
- **Civil/Tort Law**: Wrongs against individuals/companies resulting in damage
- **Criminal Law**: Violations of government law that was developed to protect the public; can include jail time

Legal

Forensics - Court Admissible Evidence

Value # 13



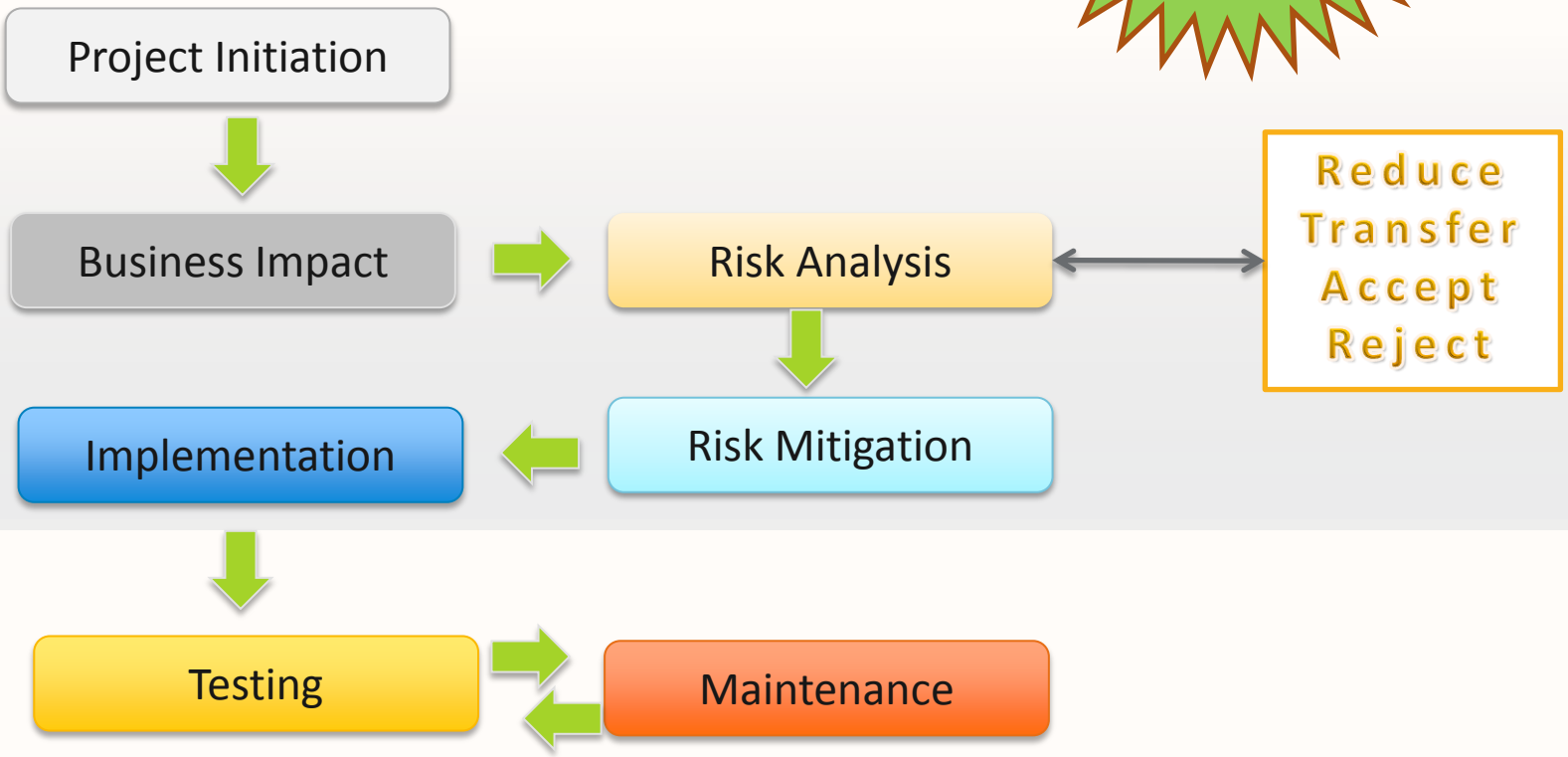
Common reason for improper evidence collection & prosecutions:

- No established IR Team / IR procedures
- Poorly written policies
- Broken chain of custody
- Lack of proper law enforcement POC

Risk Management, BCP & DRP

High-level process overview – CIA: Availability

Value # 9



Physical

CIA - Availability

Identification Mechanisms

1. Dedicated Security Guard
   Badge Reader / Ease Of Duplication
   Garage Entry

Piggybacking

2. Awareness & Trainings
   Mantraps
   Security Guard

Live Monitoring & Recording

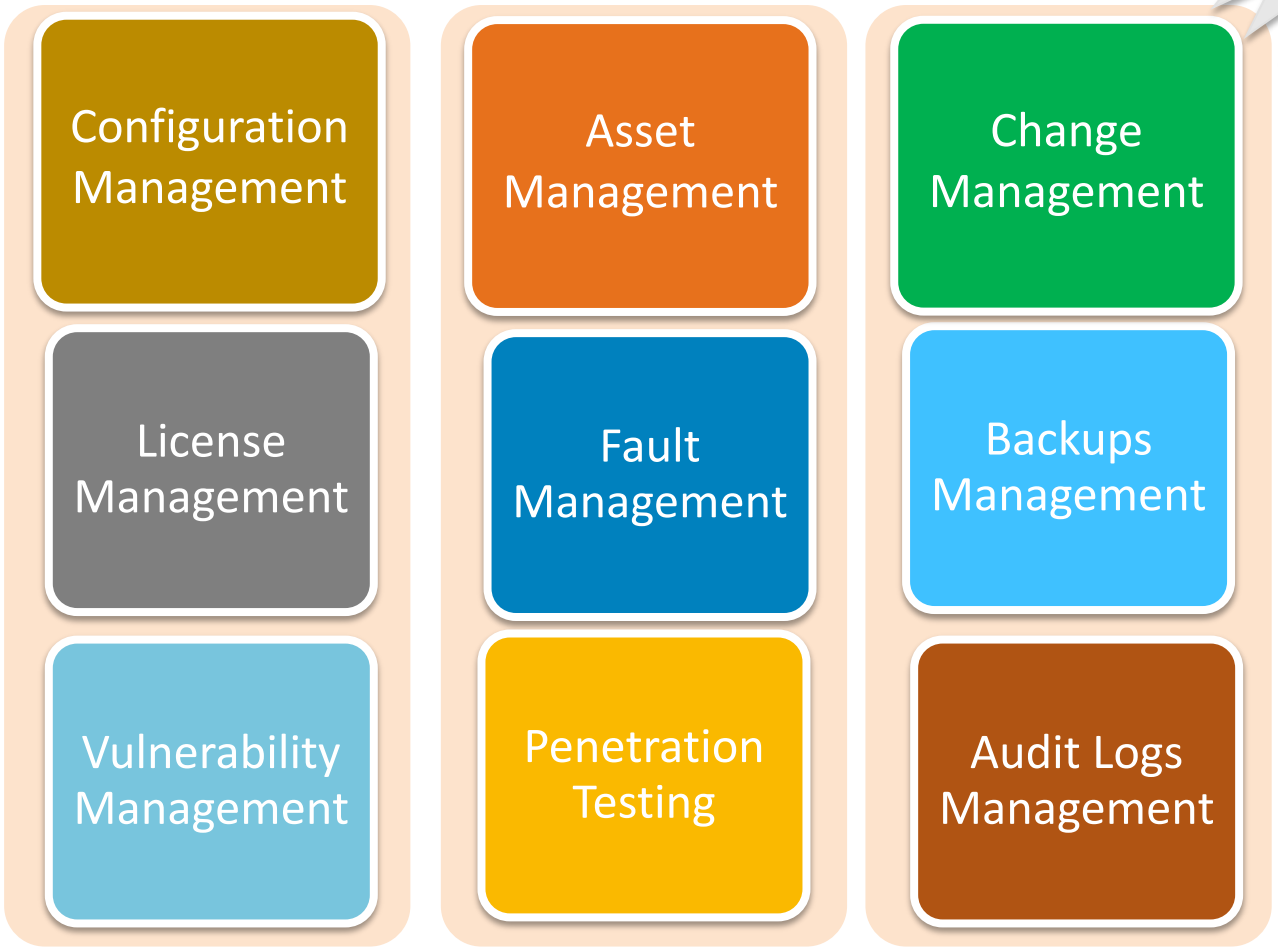
3. **What area needs to be monitored?**
   Retention policy?
   Sensitive Areas – restricted amount of widnows

- **Device Security:**
  - Locking mechanism
  - Tracing software
  - Encryption
  - Inventory system
  - Recycling procedure
  - Fencing & physical barriers
  - Fail-safe or Fail-secure
- **Audit Trails:**
  - Logs for everyone who enters & leaves the facility
  - Logs' storage policy

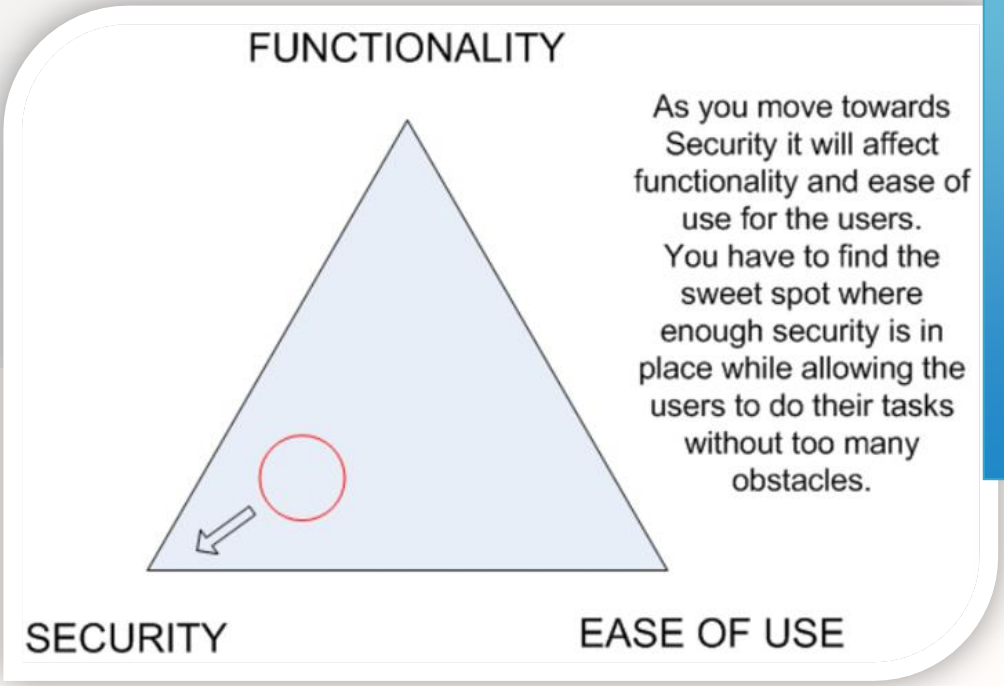
Operations Security

Someone has to do the doing…operational assurance

Value # 15



Security Goal 101:



"Fundamentally, security is a function that is supporting the business. It isn't the business itself.

Broadly speaking, the more secure you make something, the less usable it becomes. It's a bit like fast cars; the faster or more sportier you want a car to be, the less practical and useful it becomes for everyday use." - J4vv4d

THANK YOU

Reference:

- Conrad, Eric, Seth Misenar, and Joshua Feldman. *Eleventh hour CISSP study guide*. Burlington, MA: Syngress, 2011. Print.
- *Know your enemy: learning about security threats*. 2nd ed. Boston: Addison-Wesley, 2004. Print.
- Kruse, Warren G., and Jay G. Heiser. *Computer forensics: incident response essentials*. Boston, MA: Addison-Wesley, 2001. Print.
- Lucas, Julie, and Brian Moeller. *The effective incident response team*. Boston: Addison-Wesley, 2004. Print.
- Scott, Charlie, Paul Wolfe, and Bert Hayes. *Snort for dummies*. Hoboken, NJ: Wiley Pub., 2004. Print.