Information Security in Financial Institution of Nepal

By,

Er. Kumar Pudashine (MEng., AIT, Bangkok)
ISO 27001:2013, CISA, CEH,CCNP Security, JNCIA, ITIL, ActivIdentity Certified
Information Security Officer,
Information Technology Division,
Agricultural Development Bank Ltd.
Ramshahpath, Kathmandu

"NOWADAYS, HALF a trillion dollars changes hands everyday although no hands are involved and in a sense, no dollars either, and it's not even numbers really. It's just binary sequences of pulses racing between computers."

(Robert Krulwich, Economics Correspondence for National Public Radio and CBS,

quoted in New Yorkers, February 18. 1998)

Presentation Outline

- Cyber Threats in FI
- Information Security
  - Rubric Cube Model of an Information Security
  - Value and Impact
- Risks in Financial Institutions ??
- Solution Outlines
  - Information Security Management System
  - Control Objectives for Information and Related Technologies
  - Information Technology Service Management

Cyber Threats to Financial Institutions and other National Critical Infrastructure is Real and Growing at an Alarming Rate.

Estimated 40,000 Chinese Hacking groups

Average Age ~ 2X years

Income: $2-3 Million Per Year

CYBERTHREAT HEADACHES

Cyberthreats of greatest concern include...

Phishing/spear-phishing attacks

Malware (viruses, worms, trojans)

Zero-day attacks

SECURITY'S WEAKEST LINKS

These areas are rated as most difficult to secure...

Mobile devices

Social media applications

Laptop/notebooks

CARELESS EMPLOYEES

These obstacles inhibit IT from defending cyberthreats...

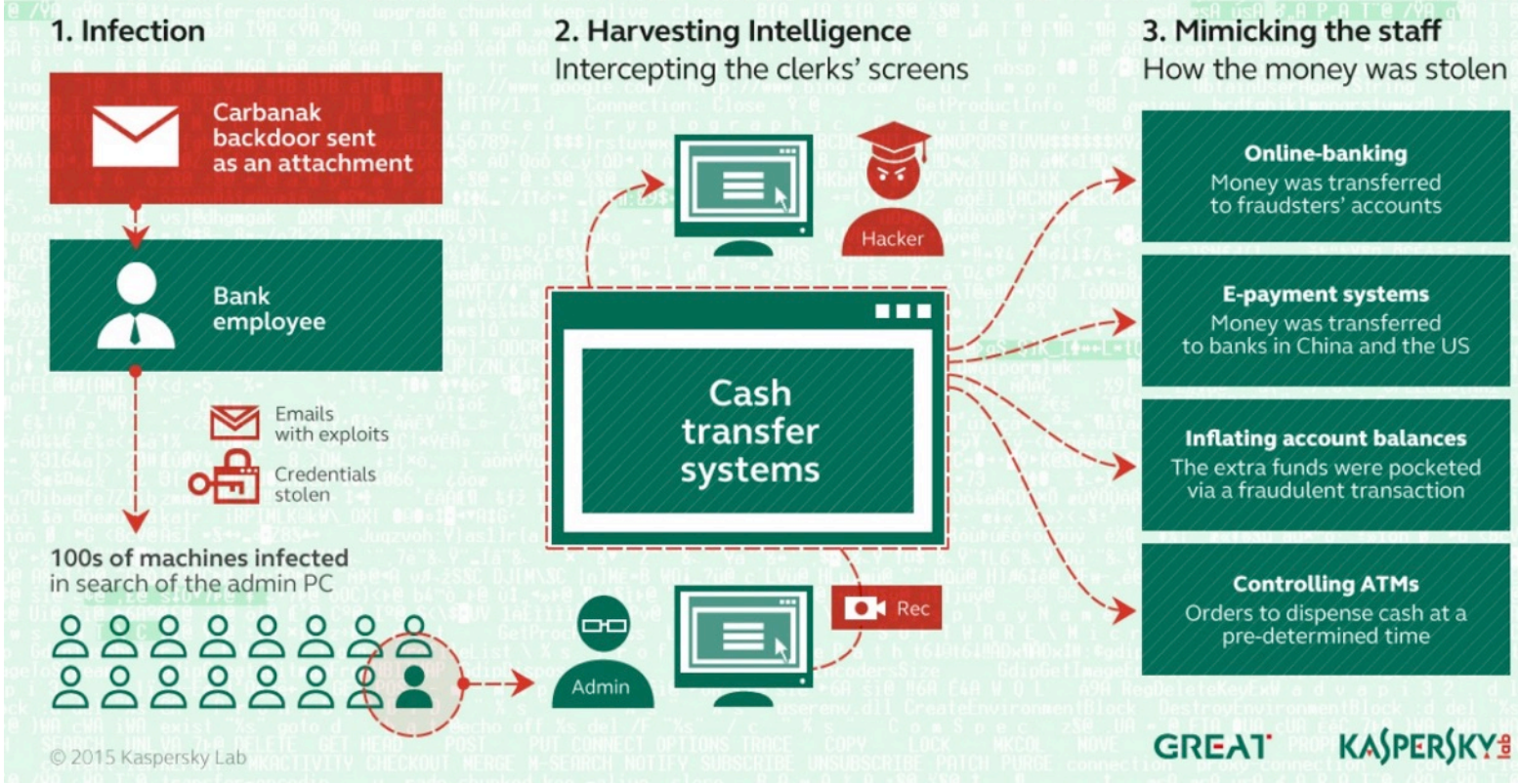
Low security awareness among employees

Lack of budget

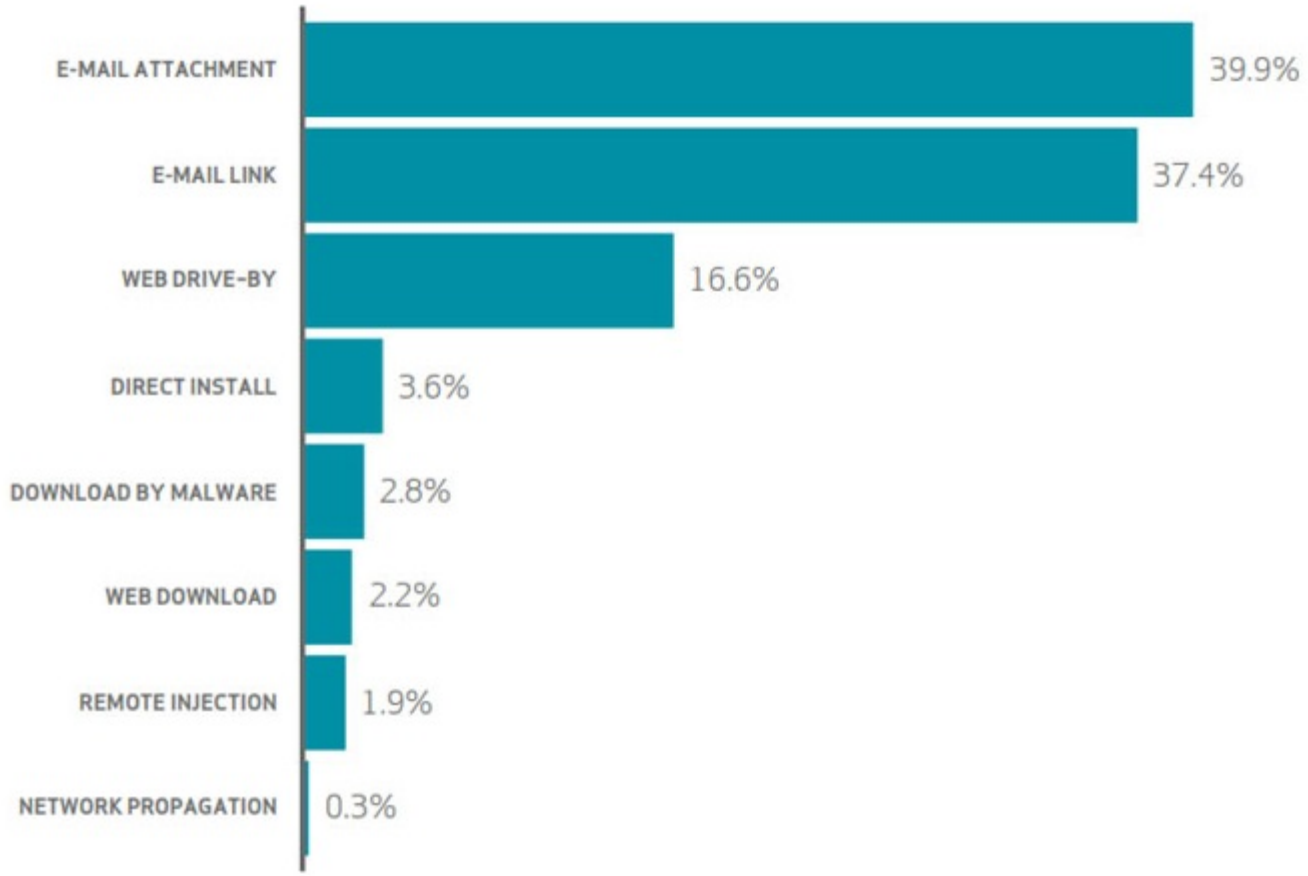
Too much data to analyze

How the Carbanak cybergang stole $1bn

A targeted attack on a bank

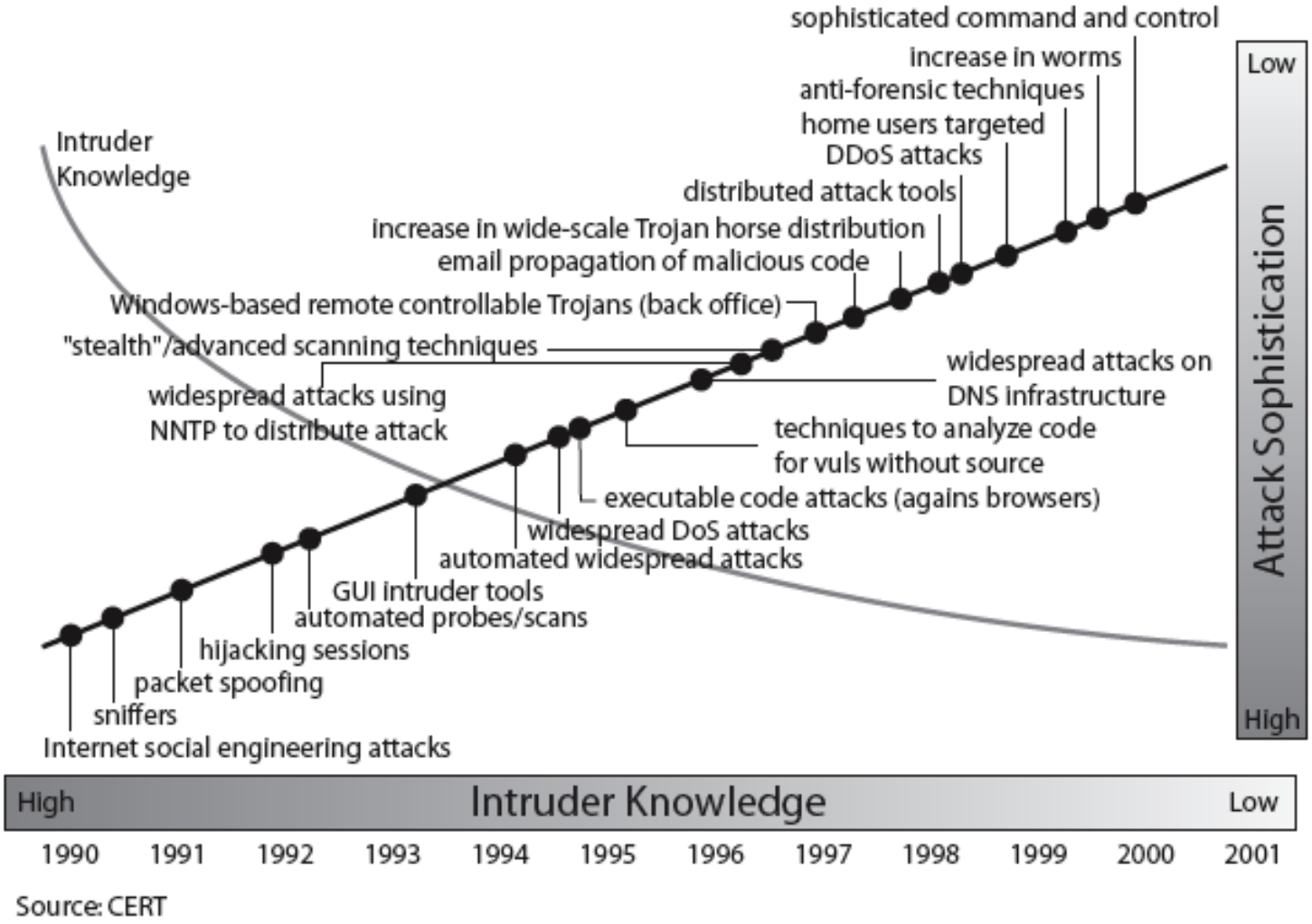


Vector of malware installation



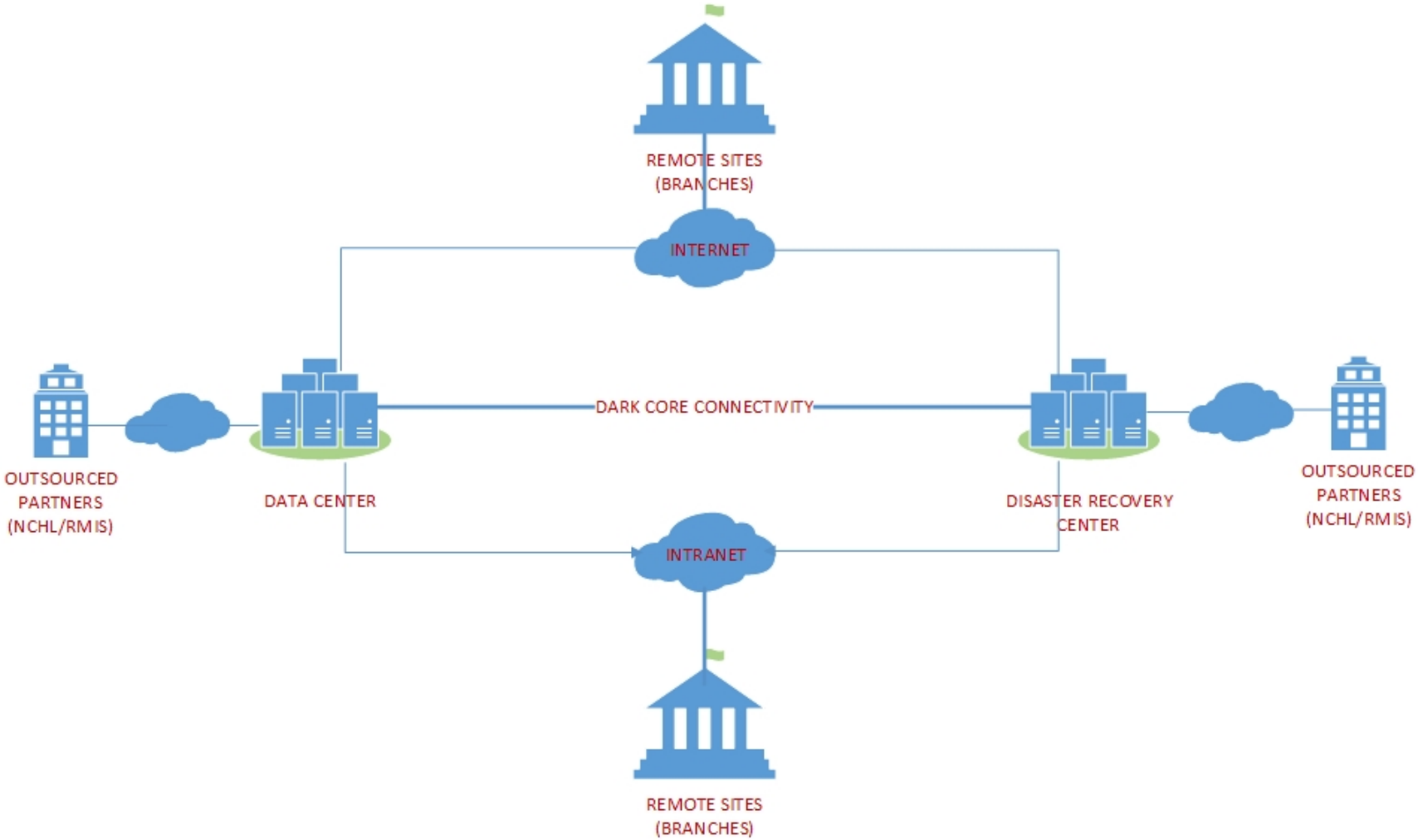
Source : Verizon Data Breach Report 2015

Intruder Knowledge vs. Attack Sophistication



Source: CERT

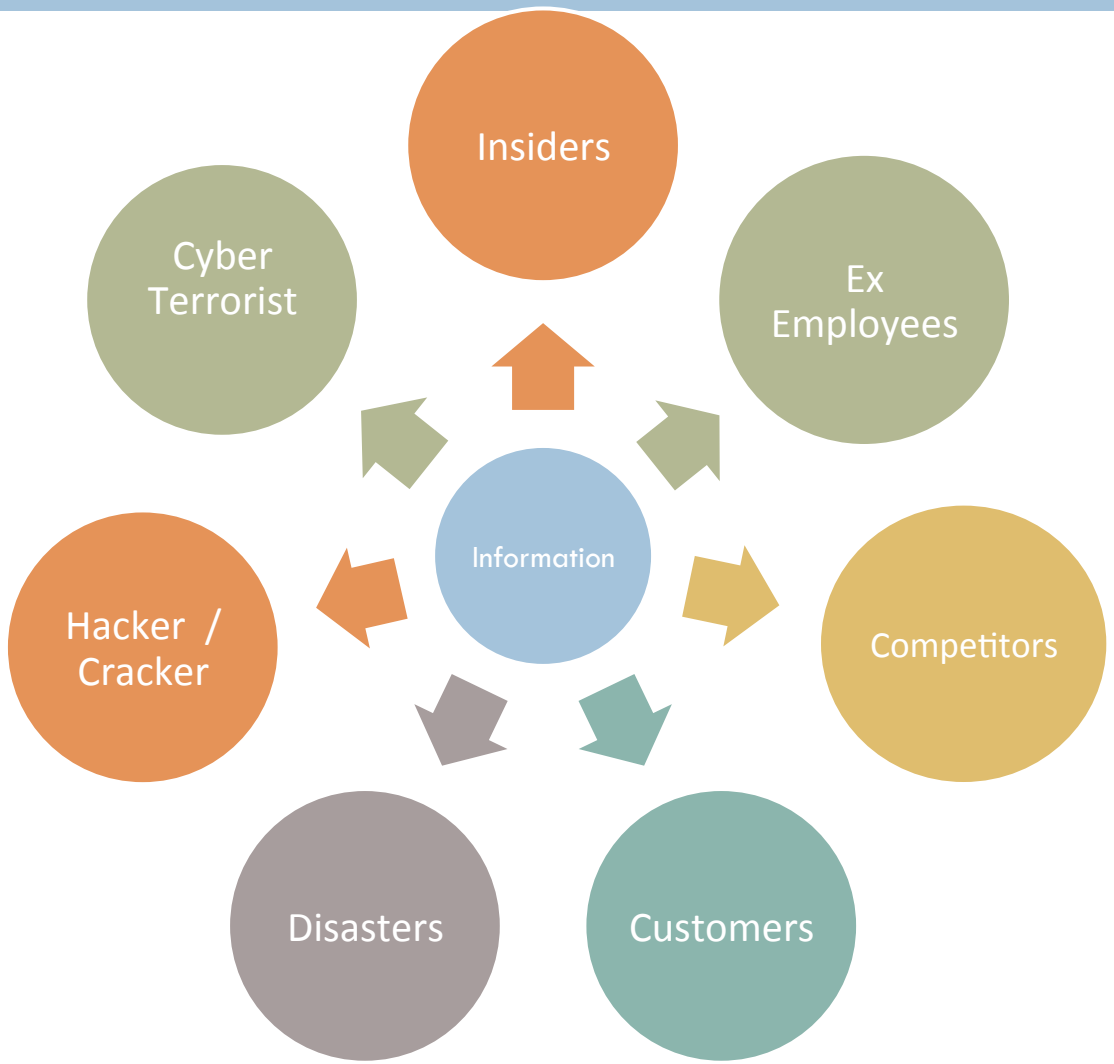
Generic FI Architecture



Risks: FI??

- Technologies
  (Data Center, Disaster Recovery Center, Core Banking System)
- Human Resources
  (Peoples: Internal & External)
- Partners
  (Outsourced Vendors)
- Process
  (Standard Operations)

Threaten of Information ?? : SS. 44 – 48,52



Information Security: Key Terms

- Information Security is a process by which Digital Information assets are Protected.

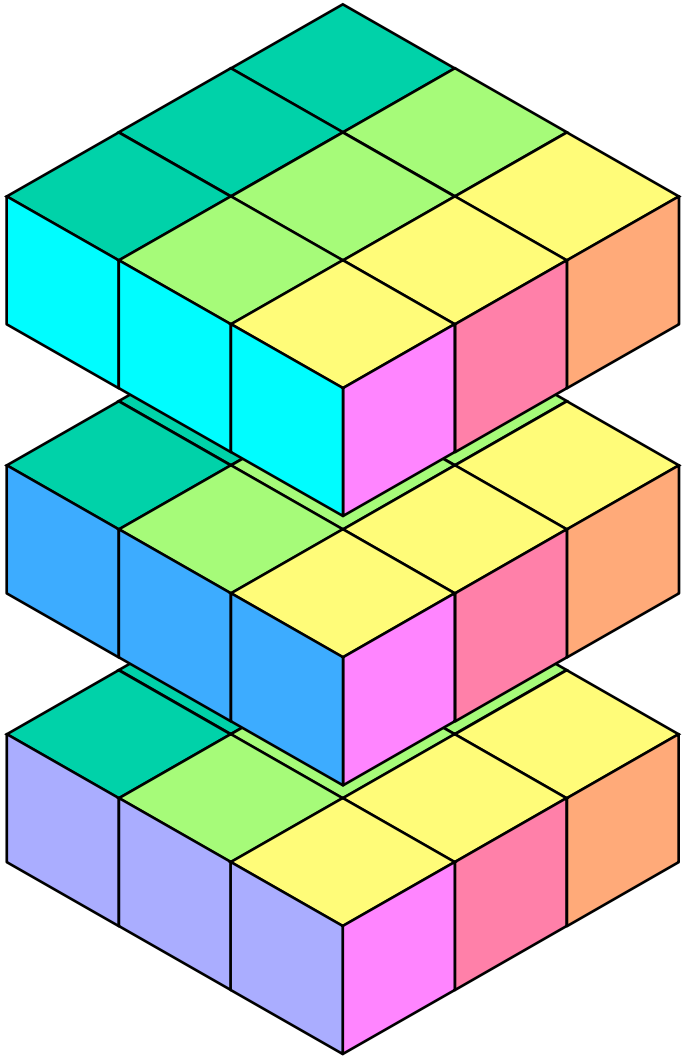
- It is not something you BUY, it is something you DO
  - It's a ***PROCESS*** not a ***PRODUCT***
- It is achieved using a combination of suitable strategies and approaches:
  - Determining the **RISKS** to information and Treating them accordingly (Proactive Risk Management)
  - Protecting **CIA** (**C**onfidentiality, **I**ntegrity and **A**vailability)
  - Avoiding, preventing, detecting and recovering from incidents
  - Securing people, processes *and* technology … not just IT!

Information Security Properties

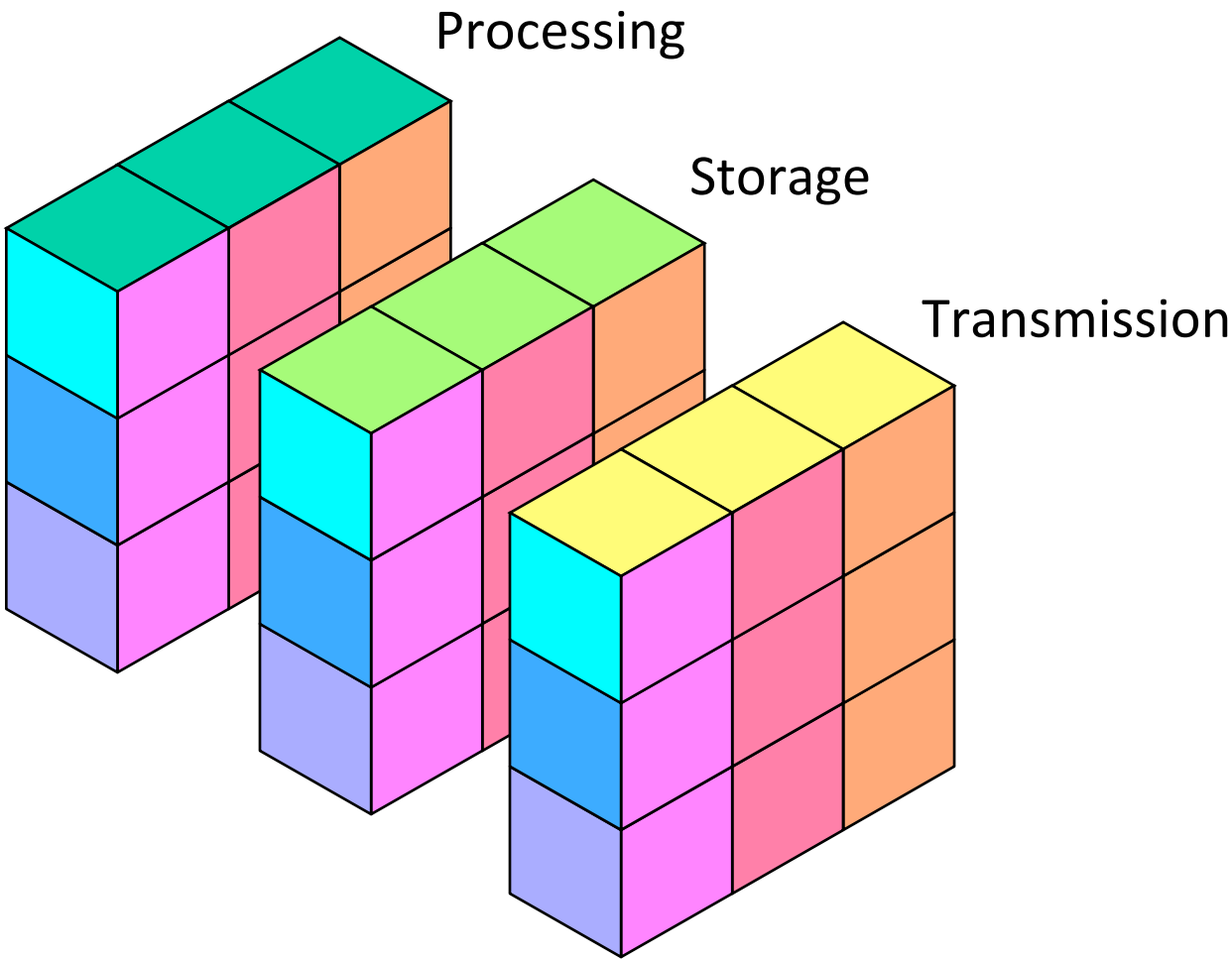
Confidentiality

Integrity

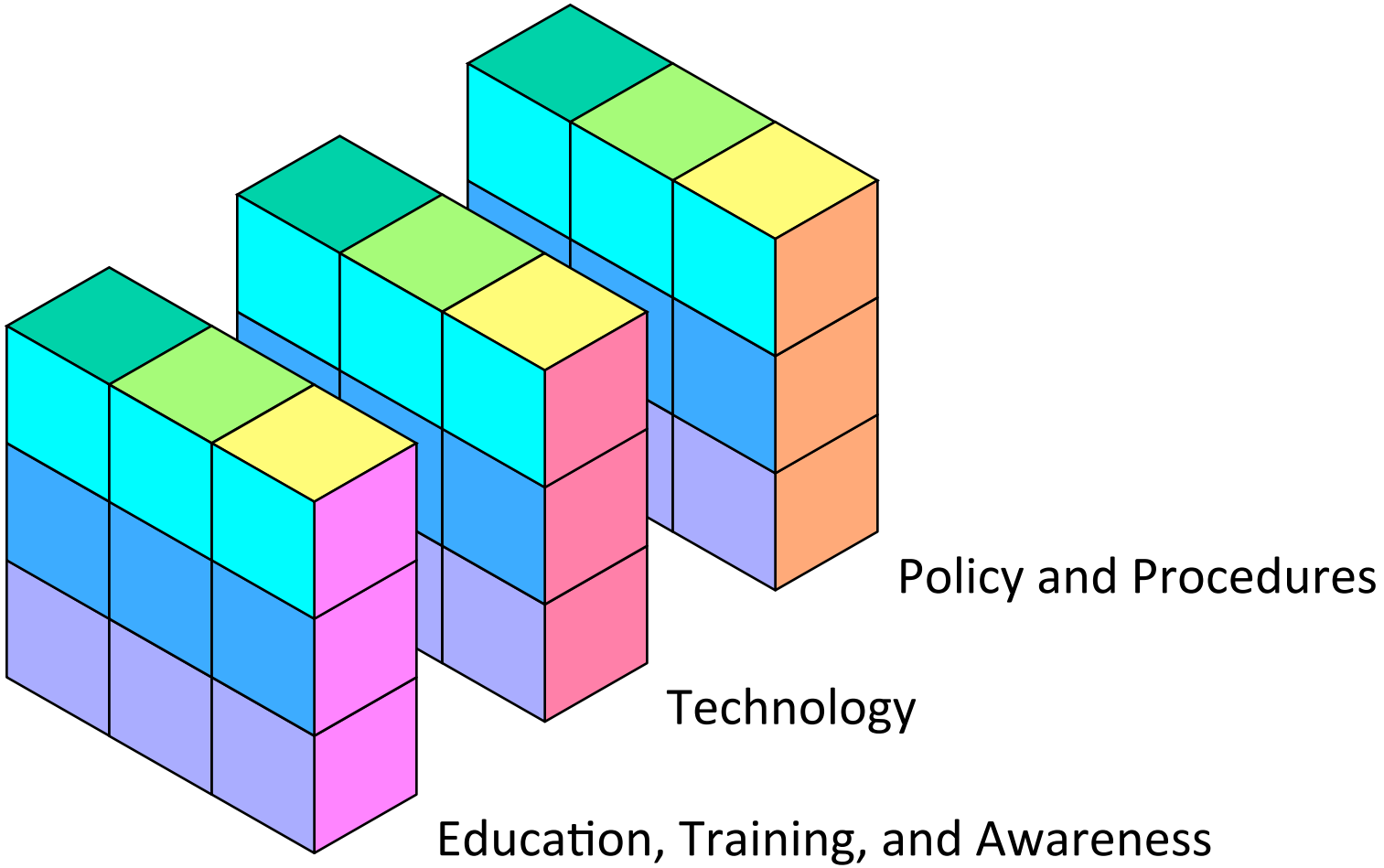
Availability



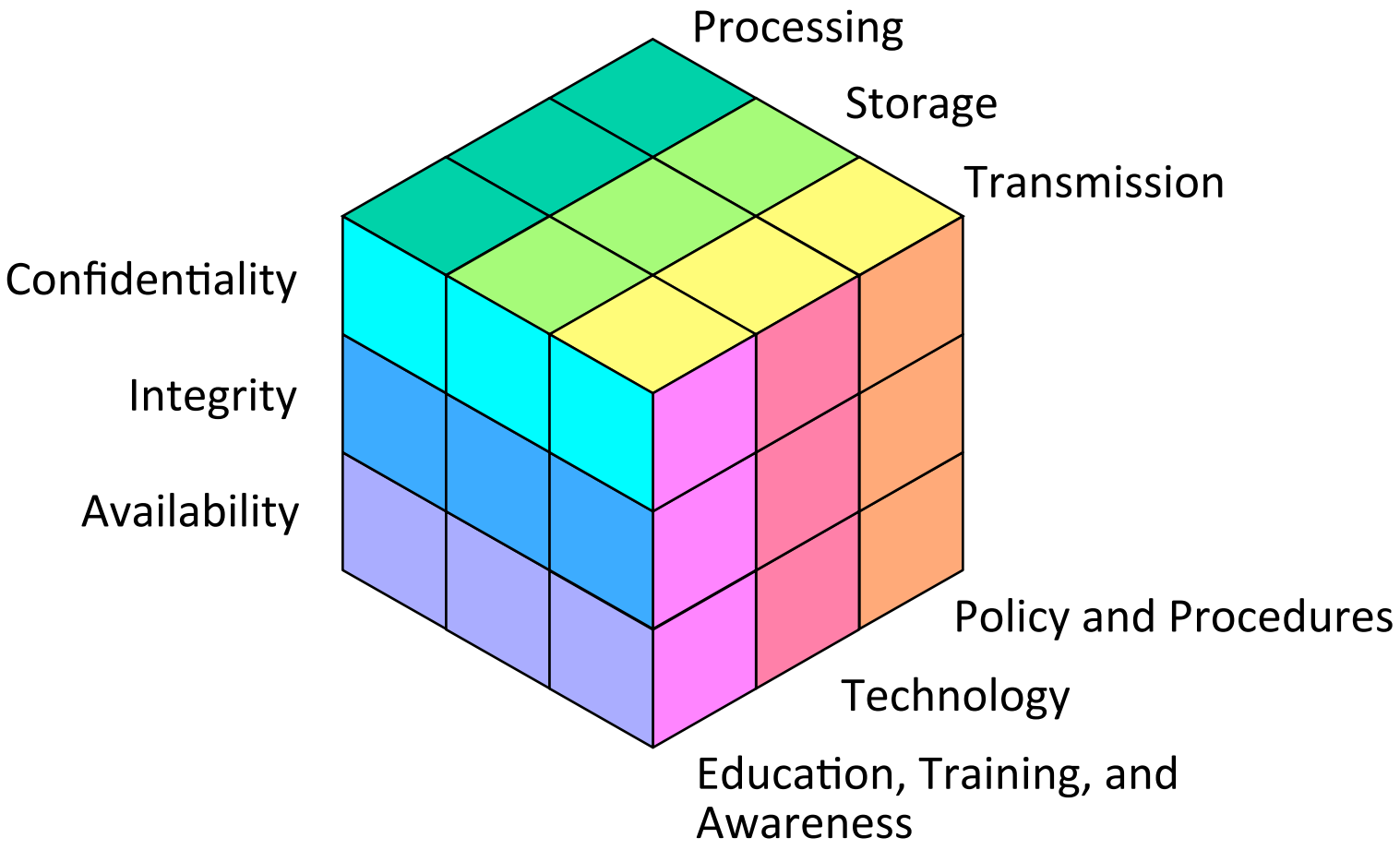
Information States



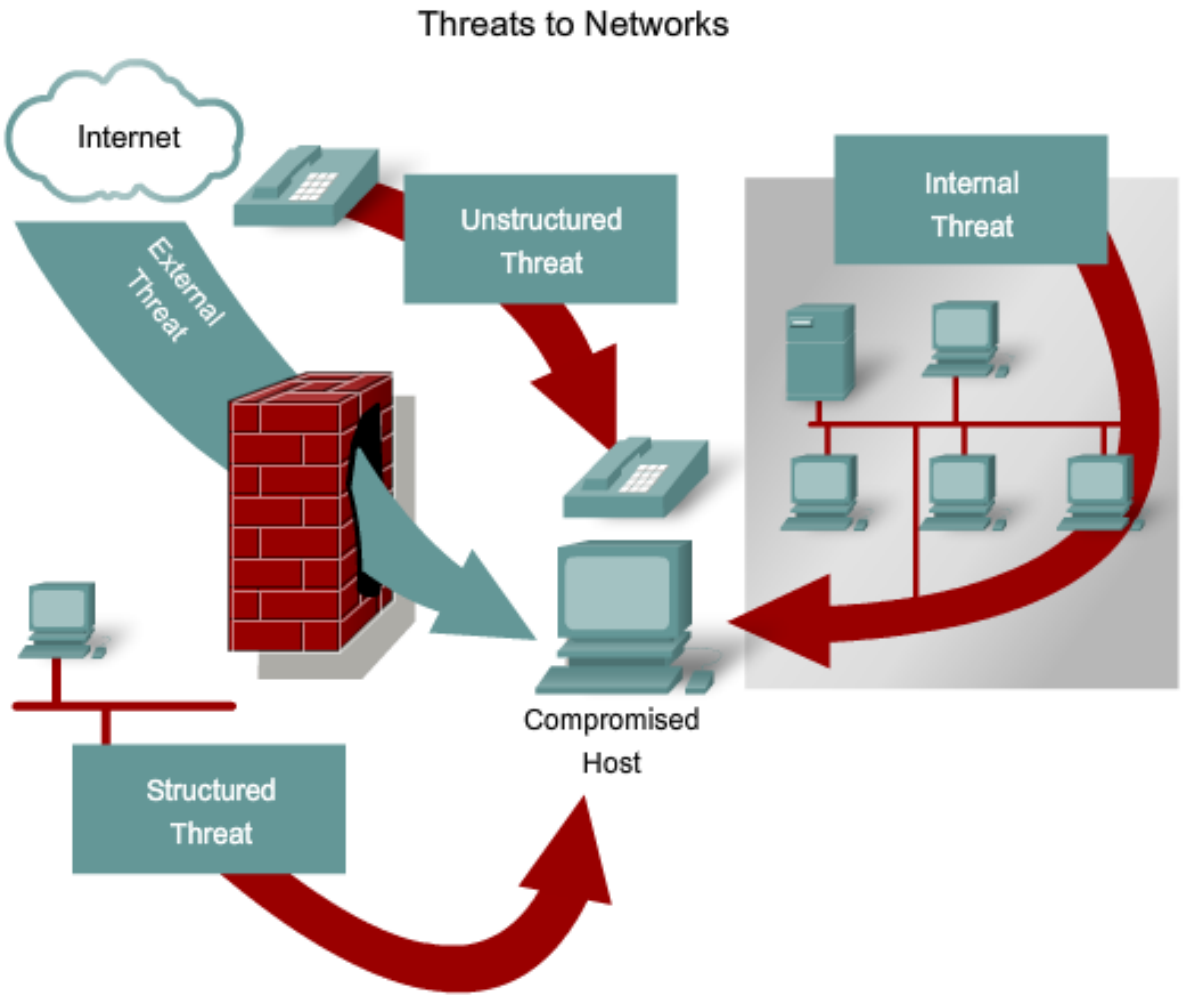
Security Measures



Information Security Model



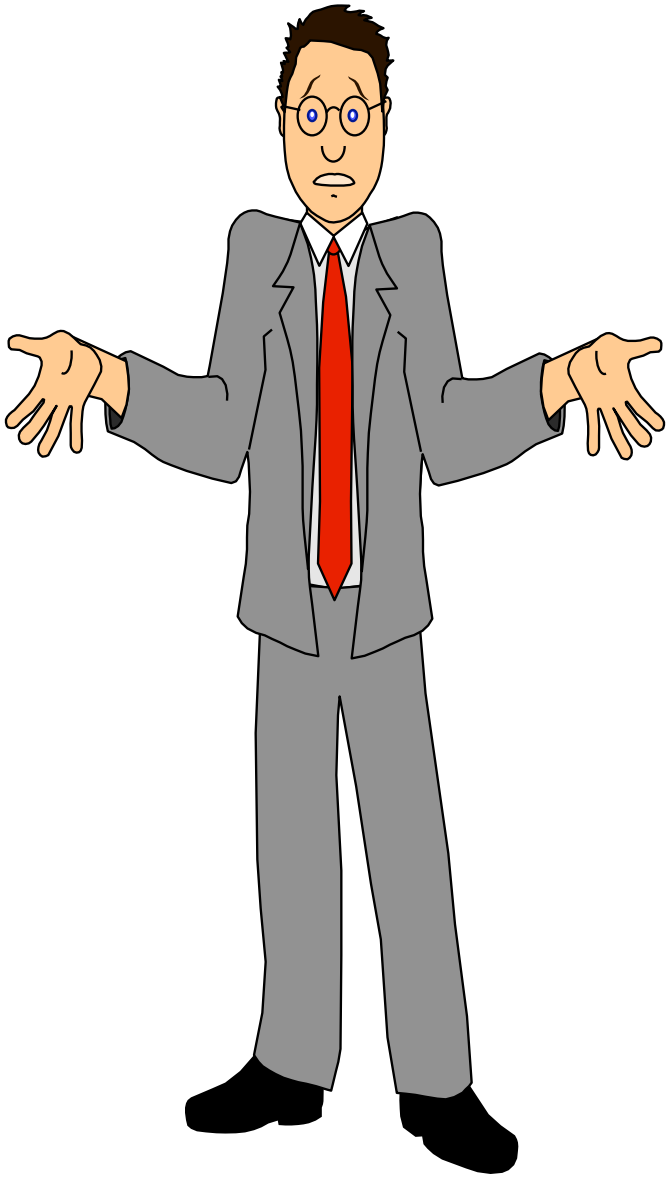
Sophistication of Threats : SS. 44 – 48,52



Information Security: Impact

- IT downtime, Business interruption
- Financial losses and costs
- Devaluation of intellectual property
- Breaking laws and regulations, leading to prosecutions, fines and penalties
- Reputation and brand damage leading to loss of customer, market, business partner or owners' confidence and lost business
- Fear, uncertainty and doubt

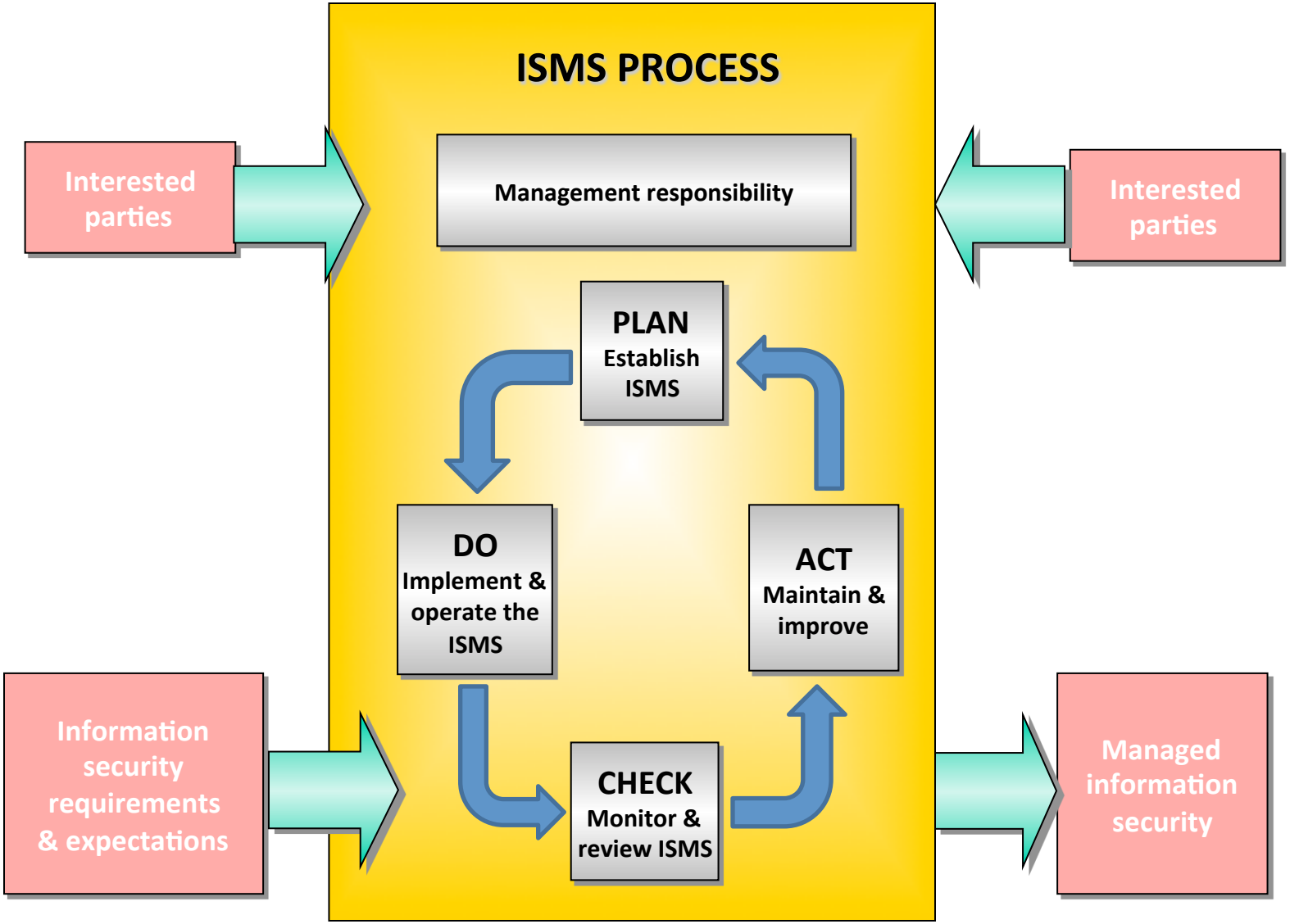
Solution Outlines?



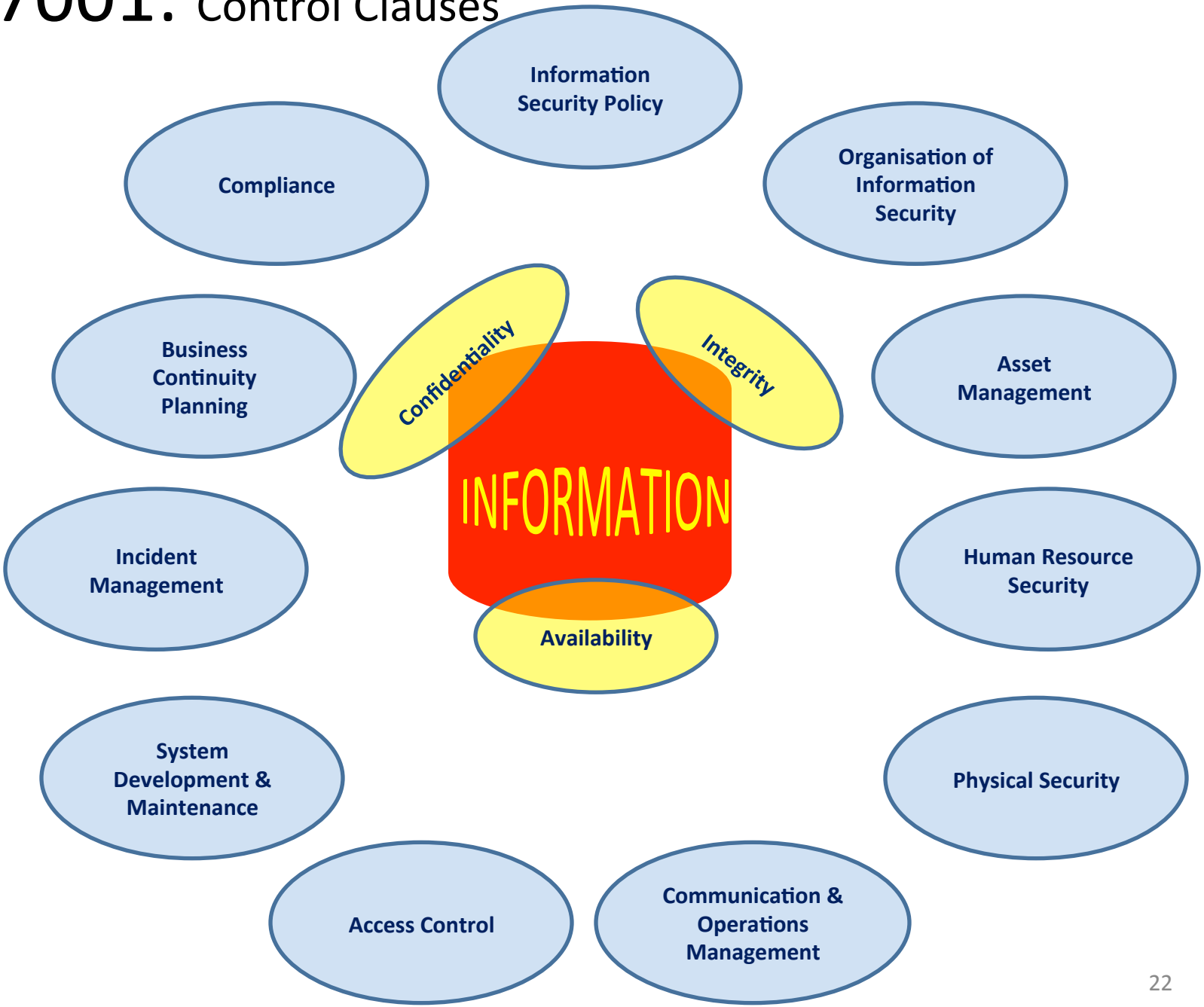
ISO: ISO 27001

- Concerns the Management of *Information* Security, not just IT/Technical security
- Formally specifies a Management System
- Uses Plan, Do, Check, Act (PDCA) to achieve, maintain and improve alignment of security with risks
- Covers all types of organizations (e.g. commercial companies, government agencies, not-for-profit organizations) and all sizes
- Thousands of organizations worldwide have been certified compliant

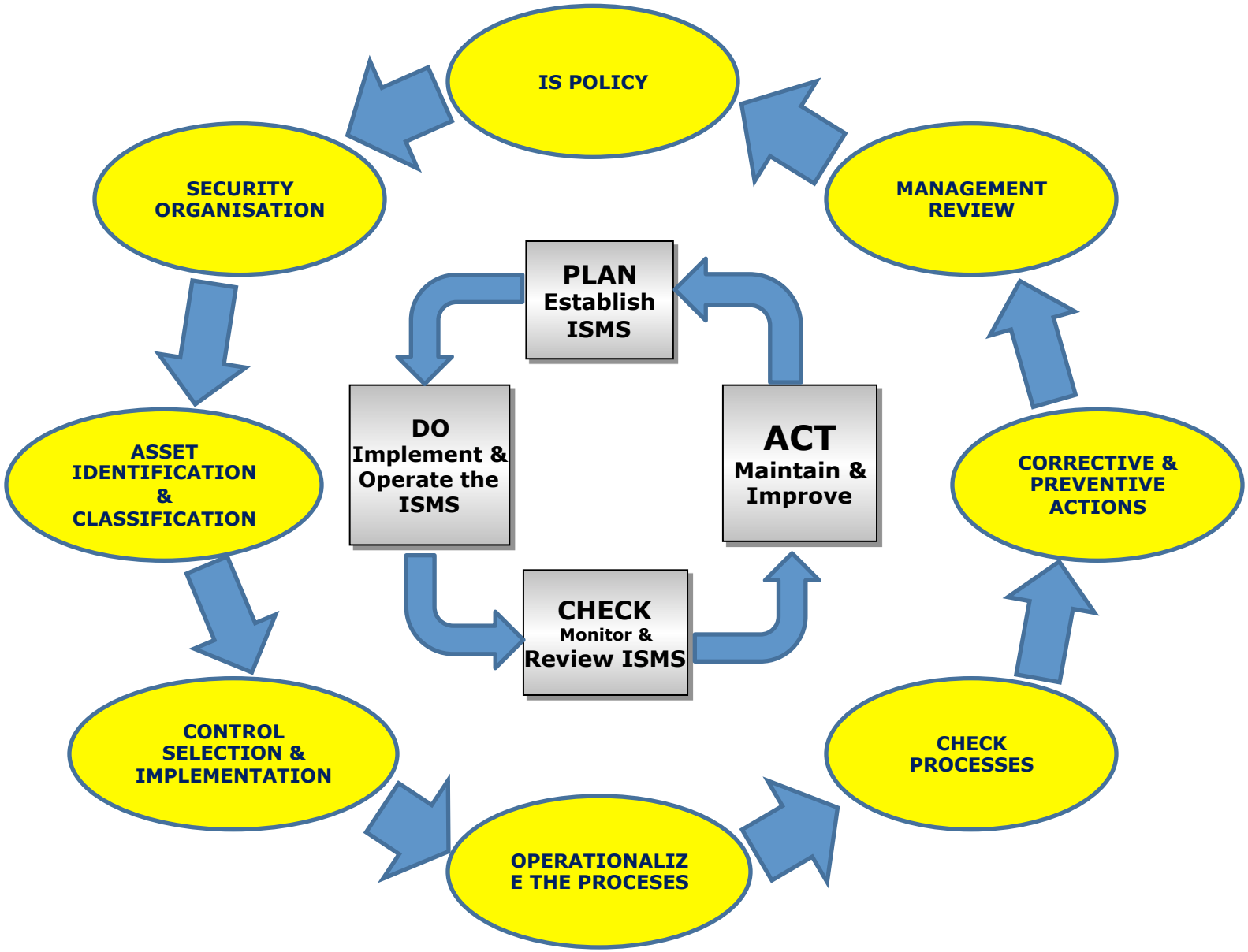
ISO 27001: PDCA



ISO 27001: Control Clauses



ISO 27001: Implementation Process Cycle



IT Governance through COBIT

(Control Objective for Information and Related Technologies)

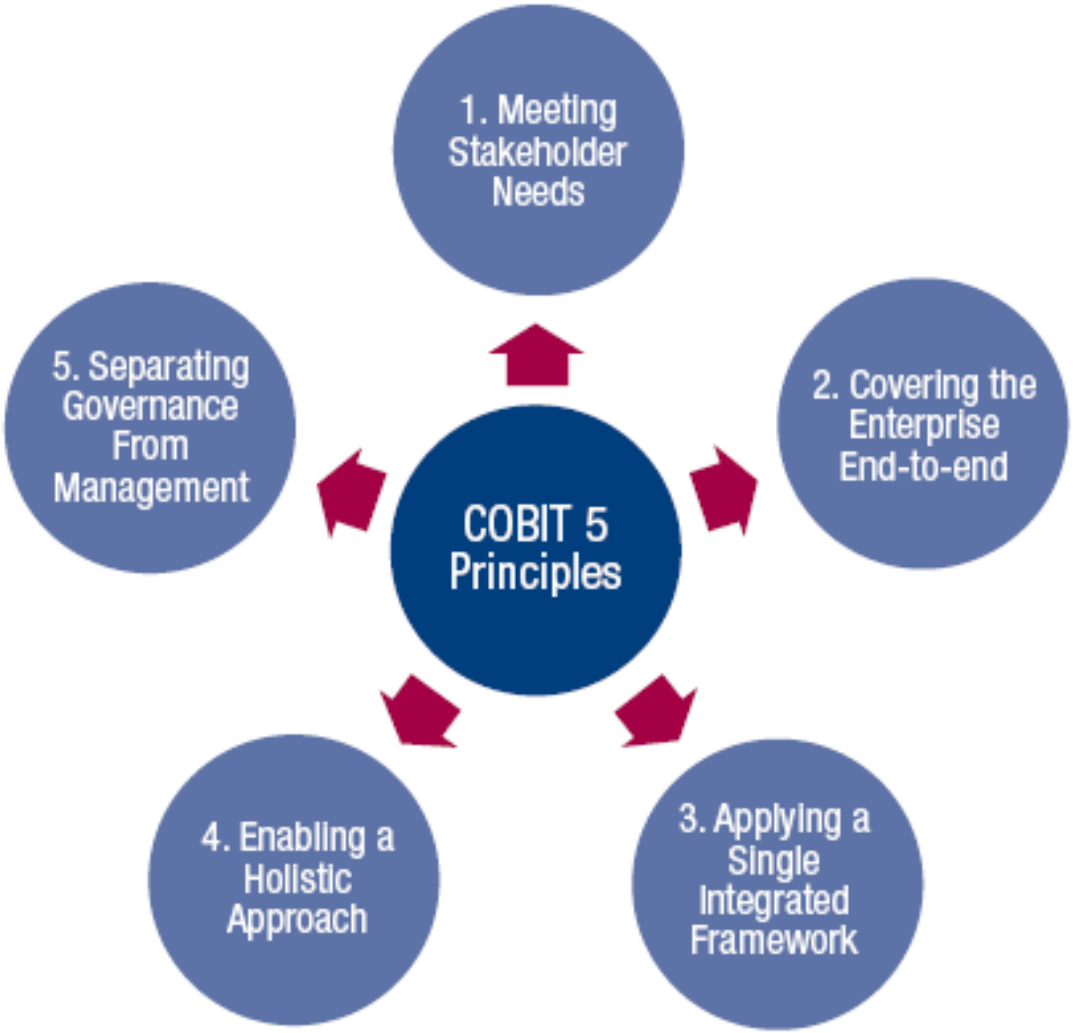
COBIT : Benefits ??

Enterprises and their executives strive to:

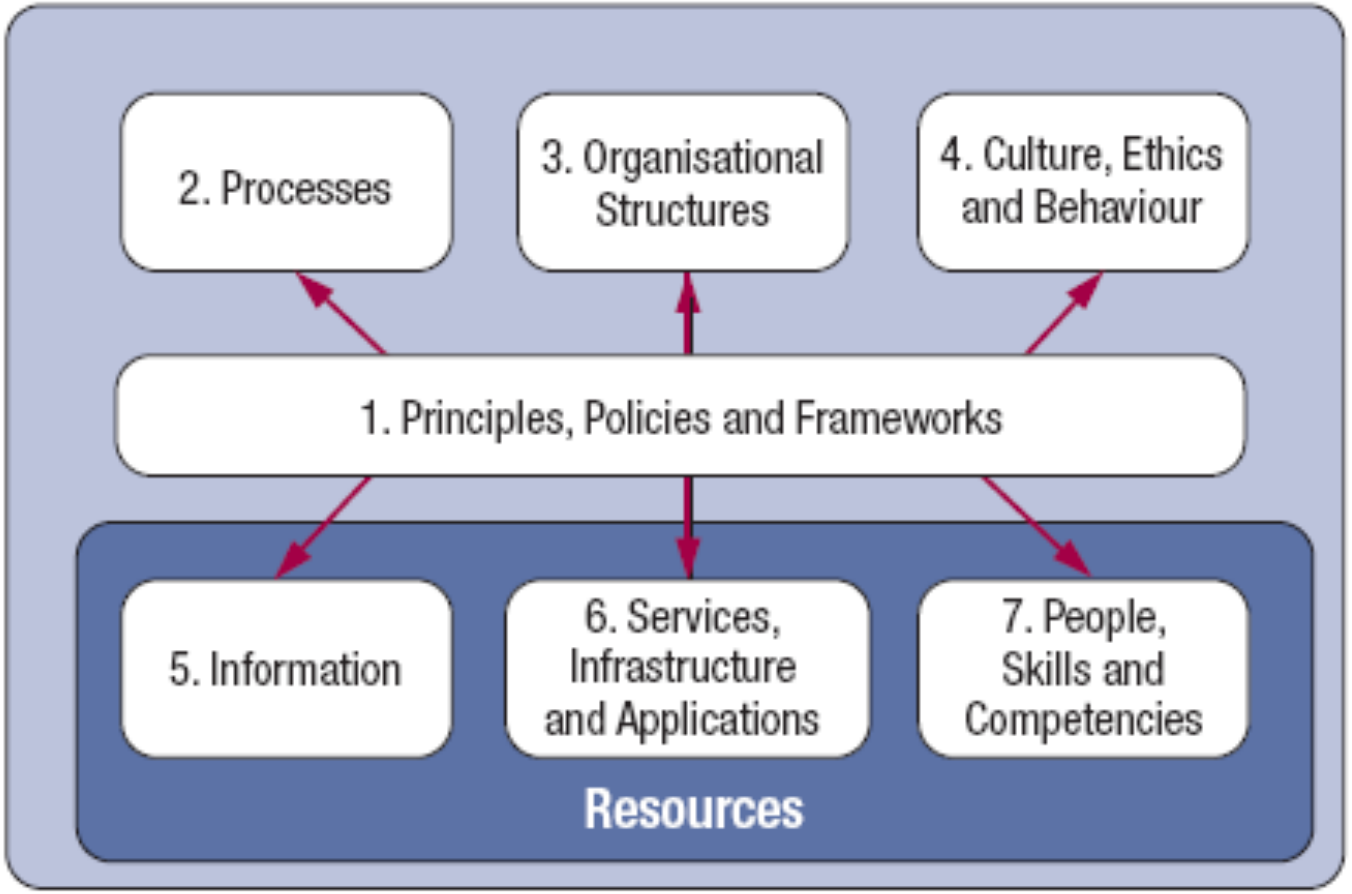
- Maintain quality information to support business decisions.
- Generate business value from IT-enabled investments, i.e., achieve strategic goals and realise business benefits through effective and innovative use of IT.
- Achieve operational excellence through reliable and efficient application of technology.
- Maintain IT-related risk at an acceptable level.
- Optimise the cost of IT services and technology.

How can these benefits be realised to create Enterprise Stakeholder value?

COBIT 5 Principles



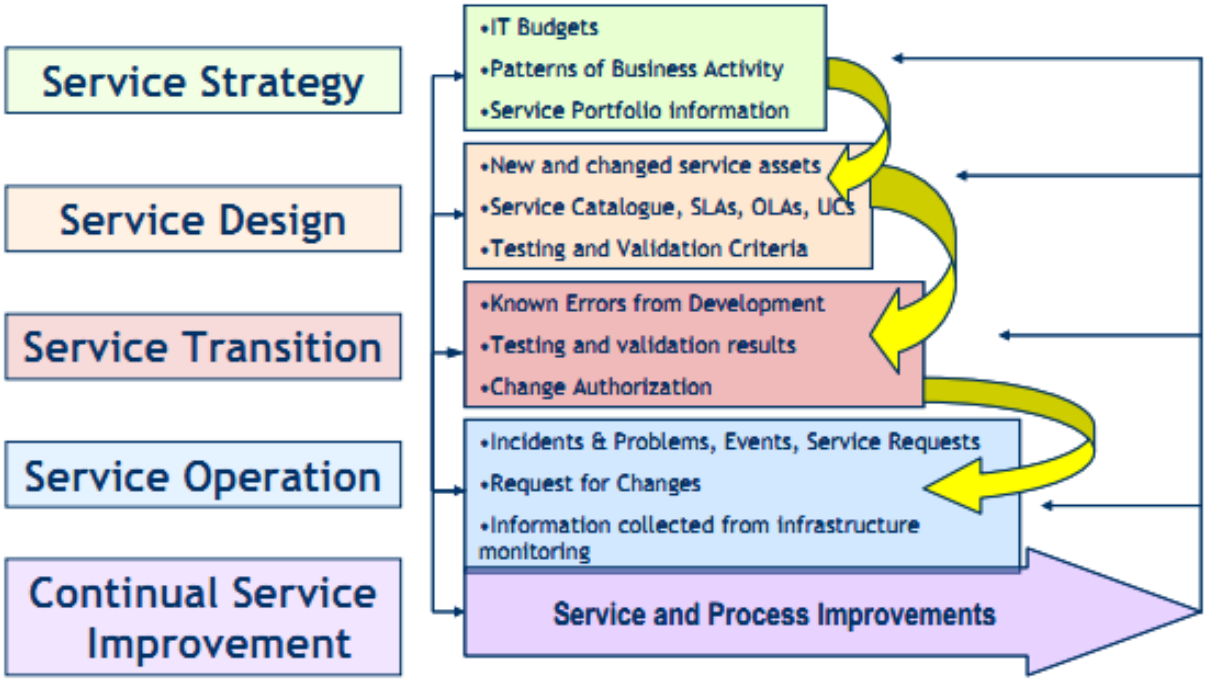
COBIT 5 Enablers



IT Service Management via ITIL

Information Technology Infrastructure Library

ITIL For: IT Service Management



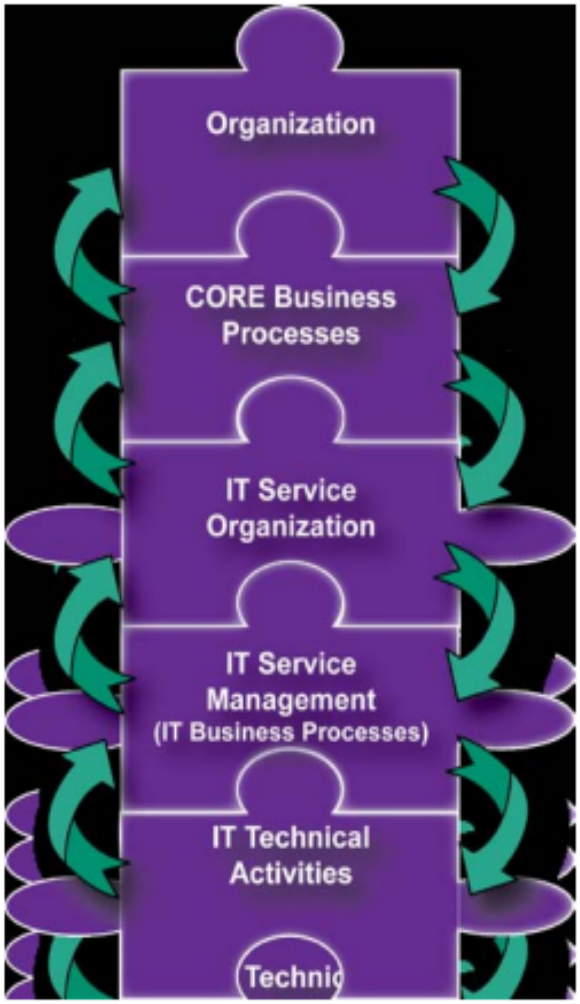
ITIL For: IT Service Management

1. ITIL® is the international de facto management framework describing "Good Practices" for IT Service Management.

1. Evolved from the UK government's efforts during the 1980s to document how successful organizations approached service management.

2. By the early 1990s they had produced a large collection of books documenting the "best practices" for IT Service Management.

3. The Office of Government Commerce in the UK continues to operate as the trademark owner of ITIL®.



Security Responsibilities: WHO ??

- Information Security Management Committee
- Senior Managements
- Information Security Manager/CISO and Department
- Incident Response Team
- Business Continuity Team
- IT, Legal/Compliance, HR, Risk and other departments
- Audit Committee
- Last but not least, **YOU..!!**

Information Security Life Cycle

References

- McLaughlin K.A., Damiano F., *American ITIL*, SIGUCCS 07, October 7-10, 2007, Orlando, Florida, USA
- Parker J., *Three Key Ingredients to Effective IT Management*, Open Water Solutions, May 6, 2005
- Reddy I., Lietzell D., *Overview of ITIL at Cisco*, May 2009
- ISO/IEC 27001, *Information Security Management Systems*, October 1, 2013
- Available Online : http://www.isaca.org/cobit
- Verma S.K., Legal Dimension of Cyberspace, Indian Law Institute, New Delhi, 2004
- Sharma V., Information Technology Law and Practice (Cyber Law and E-Commerce), Universal Law Publishing, New Delhi, 2006
- Available Online : http://www.itil.co.uk
- Available Online : http://www.lawcommission.gov.np [Electronic Transaction Act, Electronic Transaction Rule, Polices]
- Available Online : http://www.nrb.org.np

Thank You