



e-Government Agency

Delivering Secure, Public-Oriented e-Government Facilities in Africa

A Holistic Approach

Dr. Jabiri Kuwe Bakari

Bsc. Computer Sc., Msc. (Eng.) Data comm., PhD.

(CEO)

e-Government Agency (eGA)



Agenda

- 1. Introduction**
- 2. e-Government Facilities in a Nutshell**
- 3. Delivering Secure, Public-Oriented e-Government Facilities**
- 4. Issues and Challenges - African perspective**
- 5. Suggestions to Address the Challenges**
- 6. Conclusion**



Introduction



e-Government

- The use of ICT , and particularly the internet, as a tool to achieve better government.
- The process involves people, hardware (computers, networks gadgets), software (operating systems and application systems) and systems (combination of hardware, software and people).
- The arrangement requires reliable and secure communication infrastructure to facilitate exchange of information, skilled staff and presence of appropriate e-legislations

e-Government Facilities

- These are general systems and components needed to create the necessary e-government offerings, such as software, hardware, infrastructure and other e-services platforms.

ICT/e-Government Security

- The protection of information systems against unauthorised access to or modification of information, whether in storage, processing or transit, and against the denial of or absence of service to authorised user or the provision of service to unauthorised users, including those measures necessary to detect, document, and counter such threats.
- It covers information, infrastructure, processes, systems, services and technology.



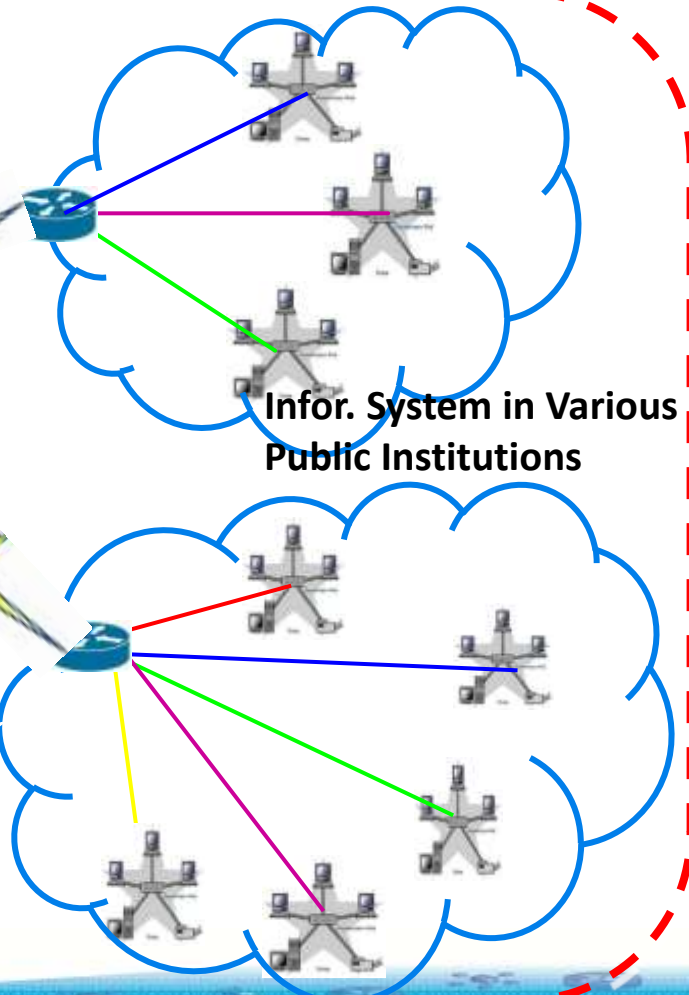
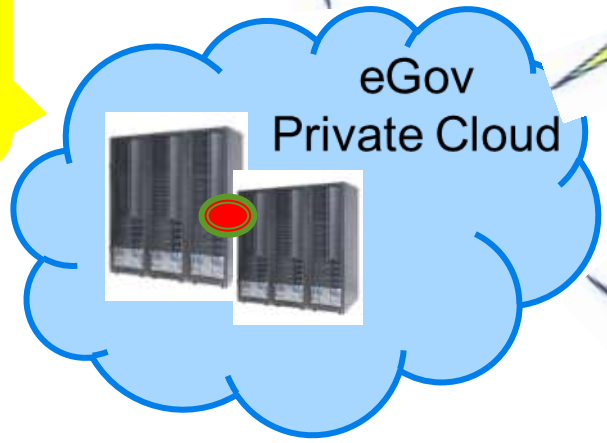
e-Government in a Nutshell



Public getting various services through Various platform / service providers / operators

Public services available through Various platform/service providers

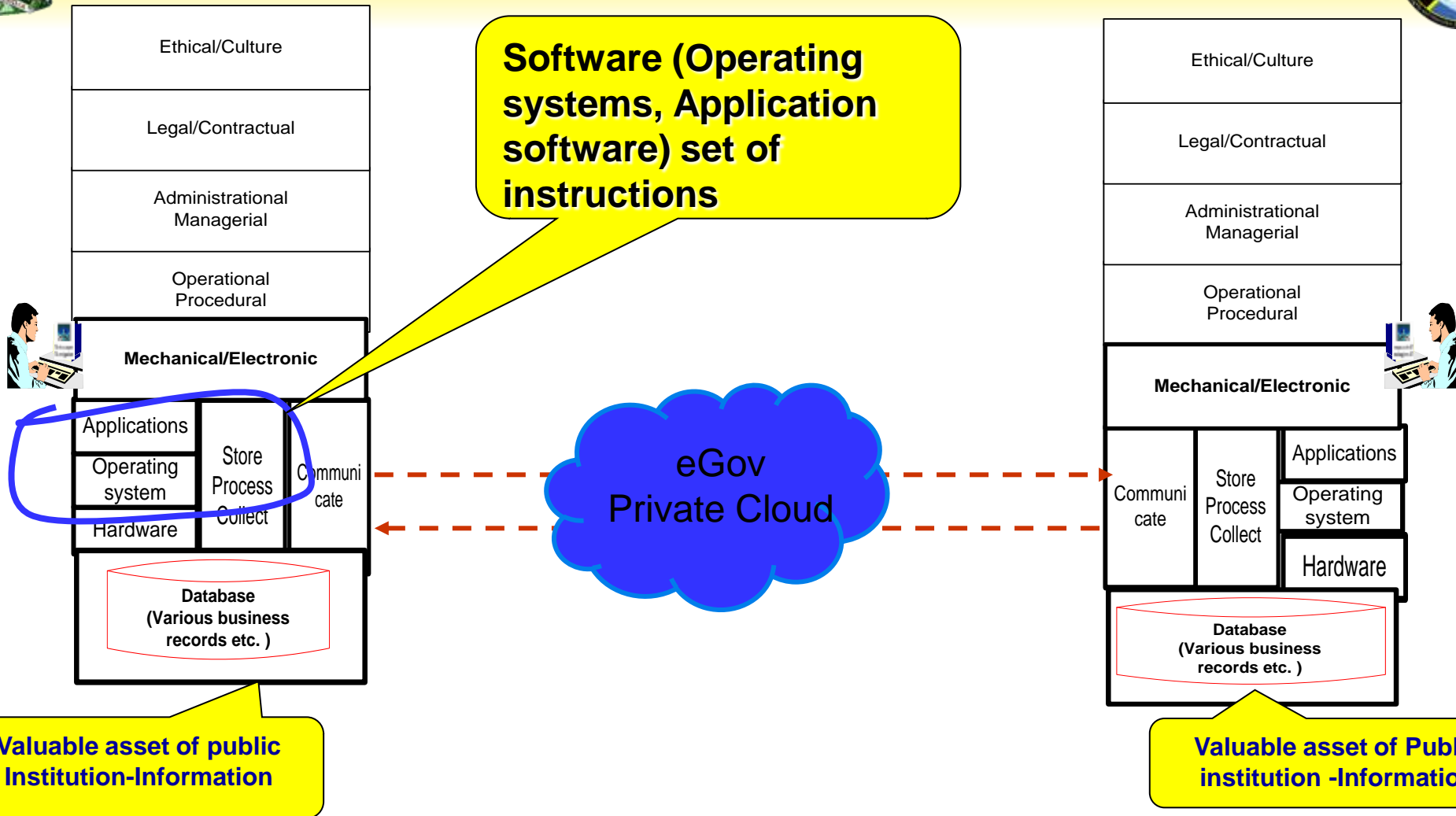
Private Cloud
Use of Shared resources, systems, Data centres, secured infrastructure etc



1-Secured information systems within The public institutions
2 Secured infrastructure between the public institutions



e-Government Facilities in a Nutshell



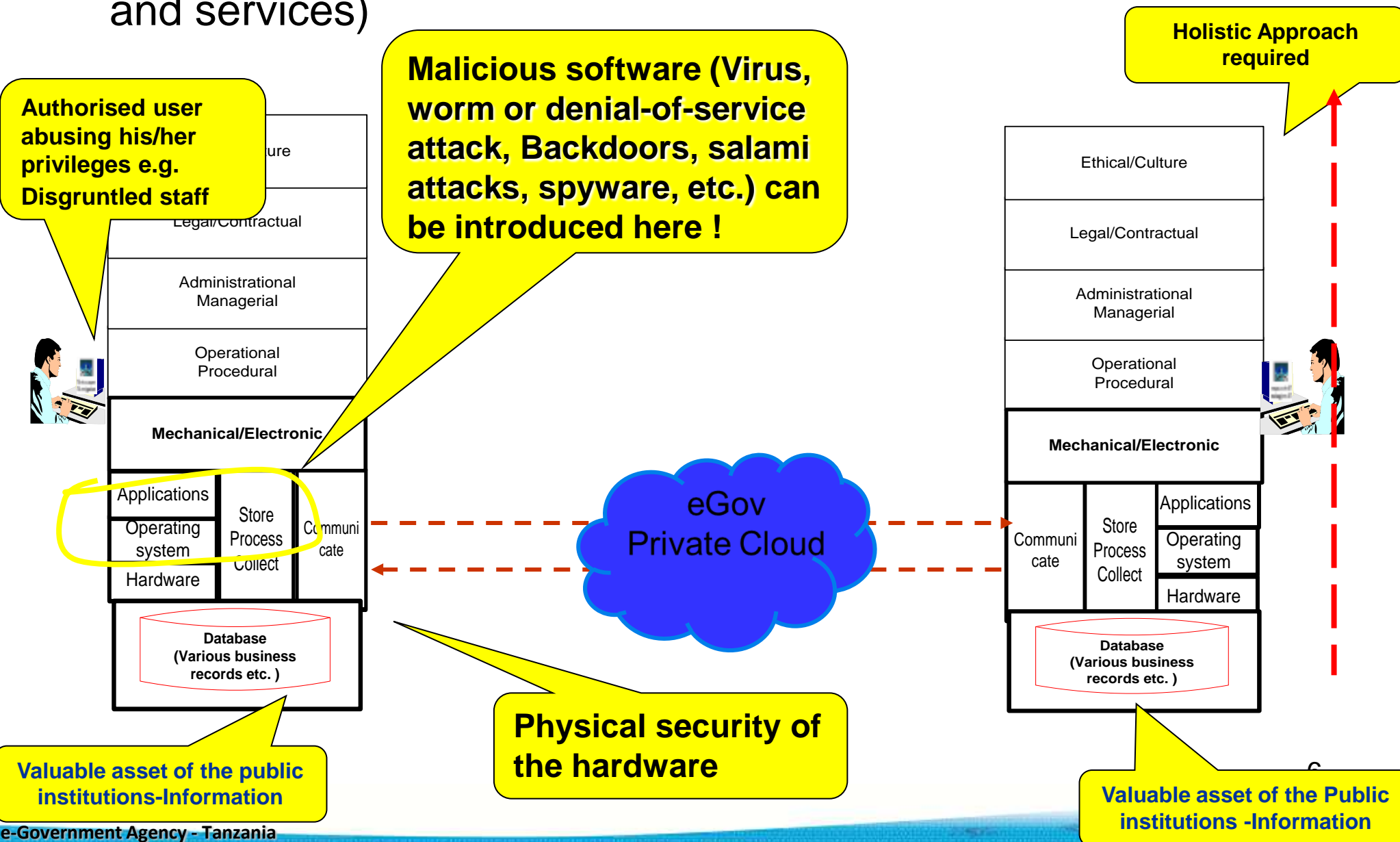
- It is about business processes, enabled by ICT, taking place within and between different public institutions
- It is about collecting, processing, storing and exchanging information within and between different public institutions



Delivering secure, public-oriented e-Government facilities



- Information security is about protection of **ICT assets/resources** in terms of **Confidentiality, Integrity and Availability** – (information and services)





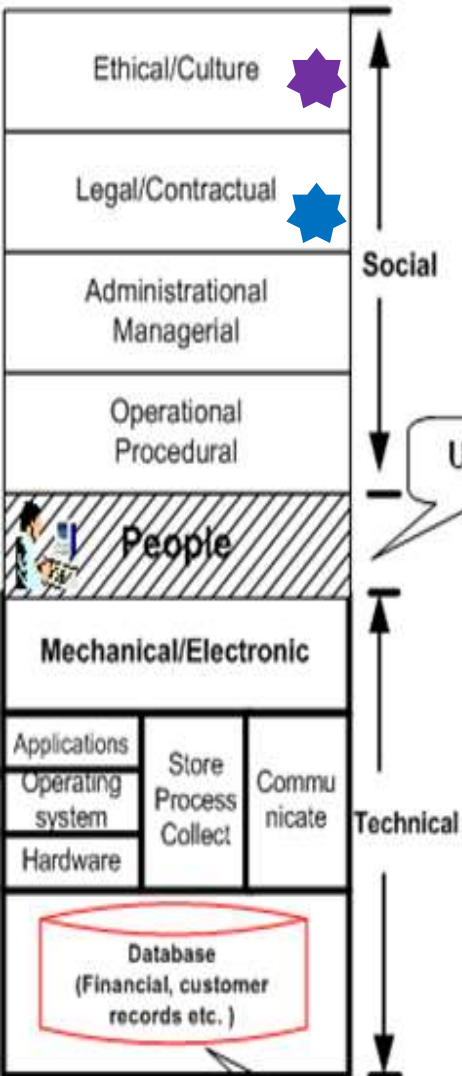
Issues and Challenges

1. Cultural and Ethical Challenges

- User behaviour - Culture of “sharing”
- Unethical behaviour,

2. Legal Challenges

- Lack of Legal framework necessary to avail e-government services to citizenry

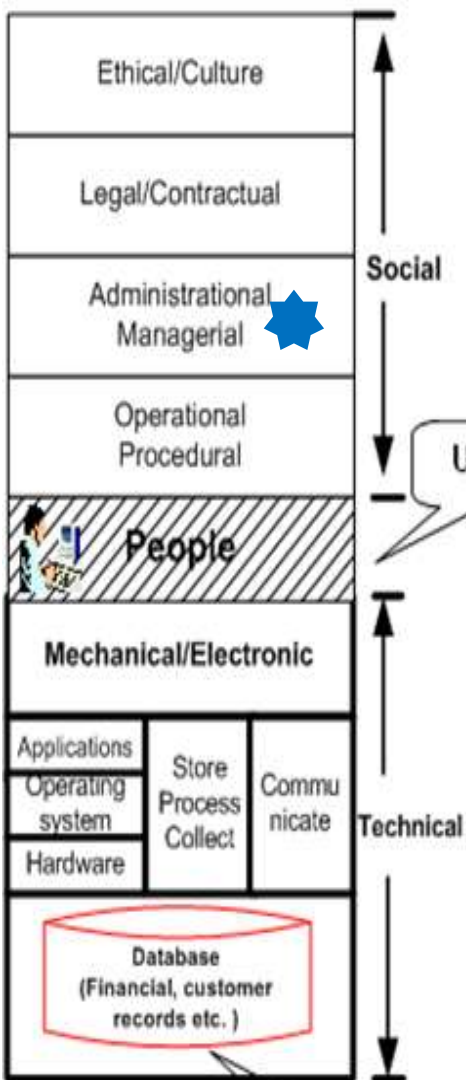




Issues and Challenges...

3. Administrative and Managerial Challenges

- Existence of perception gap between the decision makers and technical staff on ICT security. Thus, difficult in getting Strategic Management's Backing.
- Inadequacy of well structured ICT departments/units, with appropriate skills and strategically positioned within public institutions.
- Lack of competent and vetted human resource to effectively deal with ICT security.
- Inadequate collaboration between the ICT departments in public institutions and the e-Government entity
- Acquisition of e-government solutions which are not derived from institutions requirement (vendor driven)





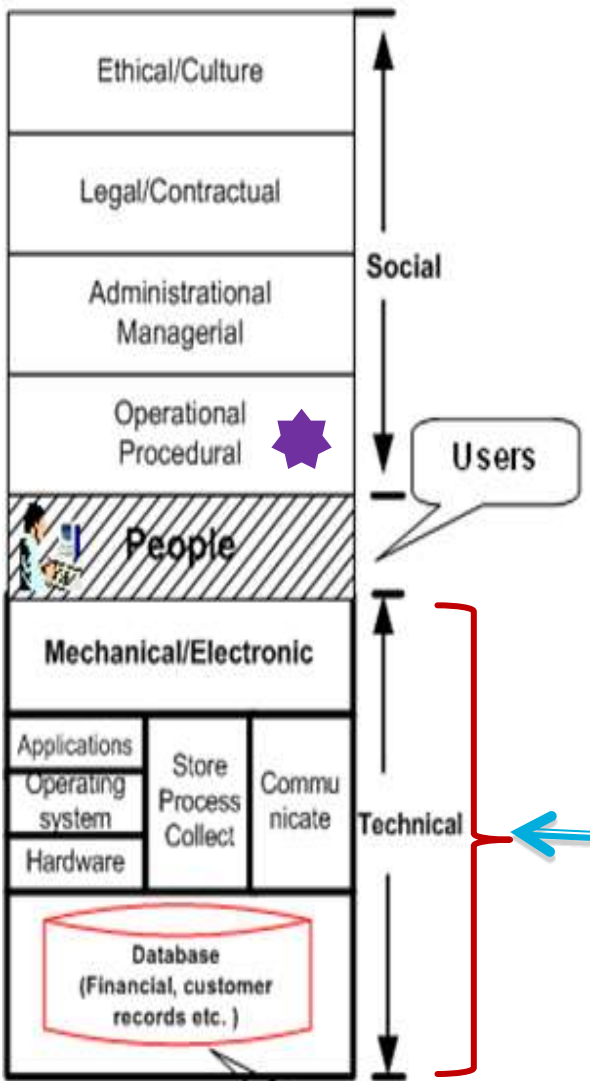
Issues and Challenges...

4) Operational Procedure Challenges

- Absence of ICT security policies, standards and guidelines both at national and organizational levels

5) Technical Issues

- Software, hardware and network vulnerabilities coupled with inadequate management, control and maintenance of ICT
- E-Government systems not integrated – exchange of information between one system and another system is facilitated by user





Suggestions to address the Challenges

At a Strategic Level

- **Knowing and acknowledging the problem/ issue**
- **Bridging the gap between decision makers and technical staff**
- **ICT security concerns should be addressed in the initial planning of e-government initiatives**
- **Formulating ICT Security strategies at national and organizational levels**
- **ICT security challenges should not be dealt in isolation, instead holistic approach is required.**
- **Putting in place coherent legal and regulatory frameworks - Whole process of e-Government need to be guided by sound legal and regulatory environment.**



Suggestions to address the Challenges

At Tactical and Operational Level

- **HR: Involving skilled and ethical personnel during acquisition, installation and operationalization of e-government**
- **Capacity building and awareness raising**
- **Implementing ICT Security strategies at national and organizational levels**
- **Use Standards and Best Practices**

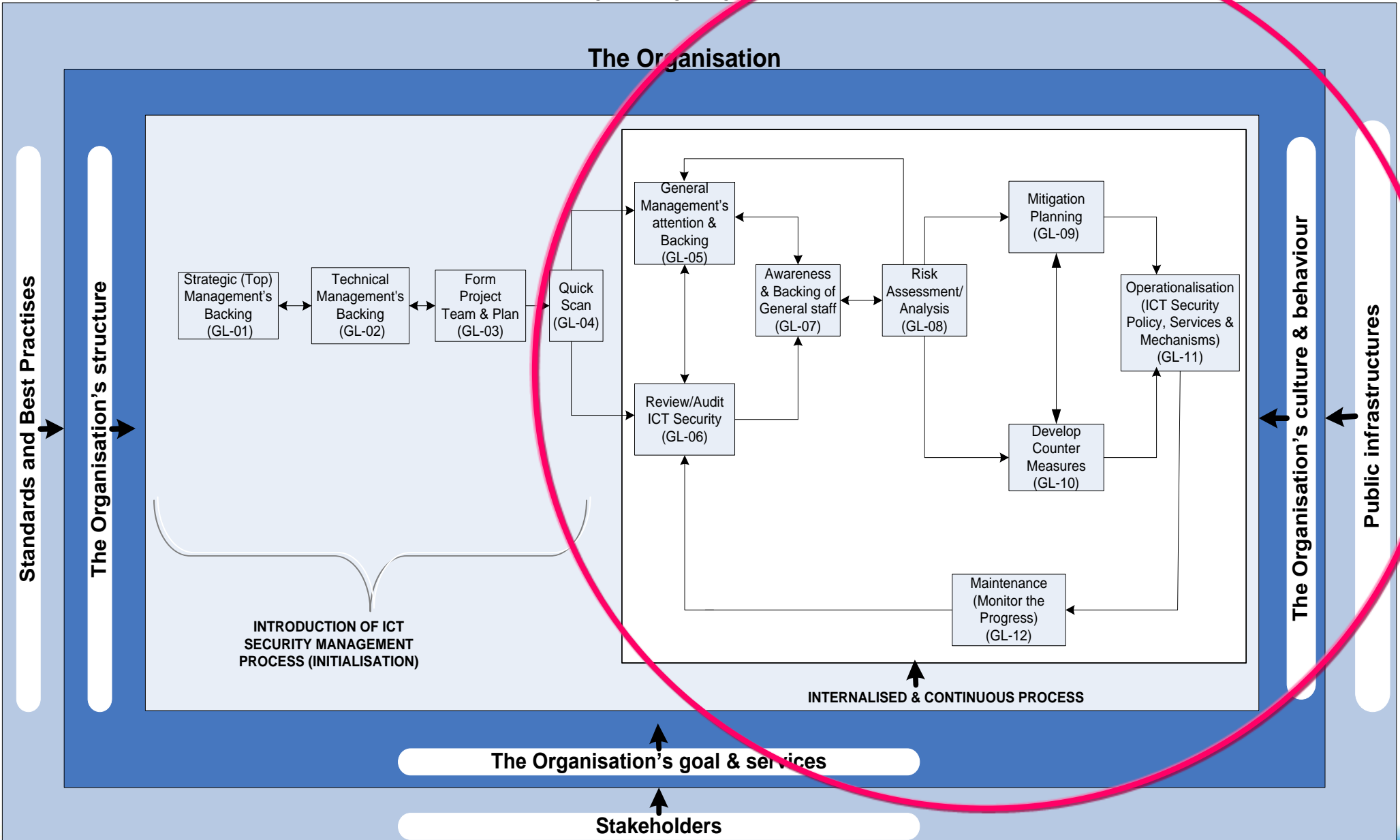


A Holistic Approach for Managing ICT Security in Organisations

Presented in a book: ISBN Nr 91-7155-383-8

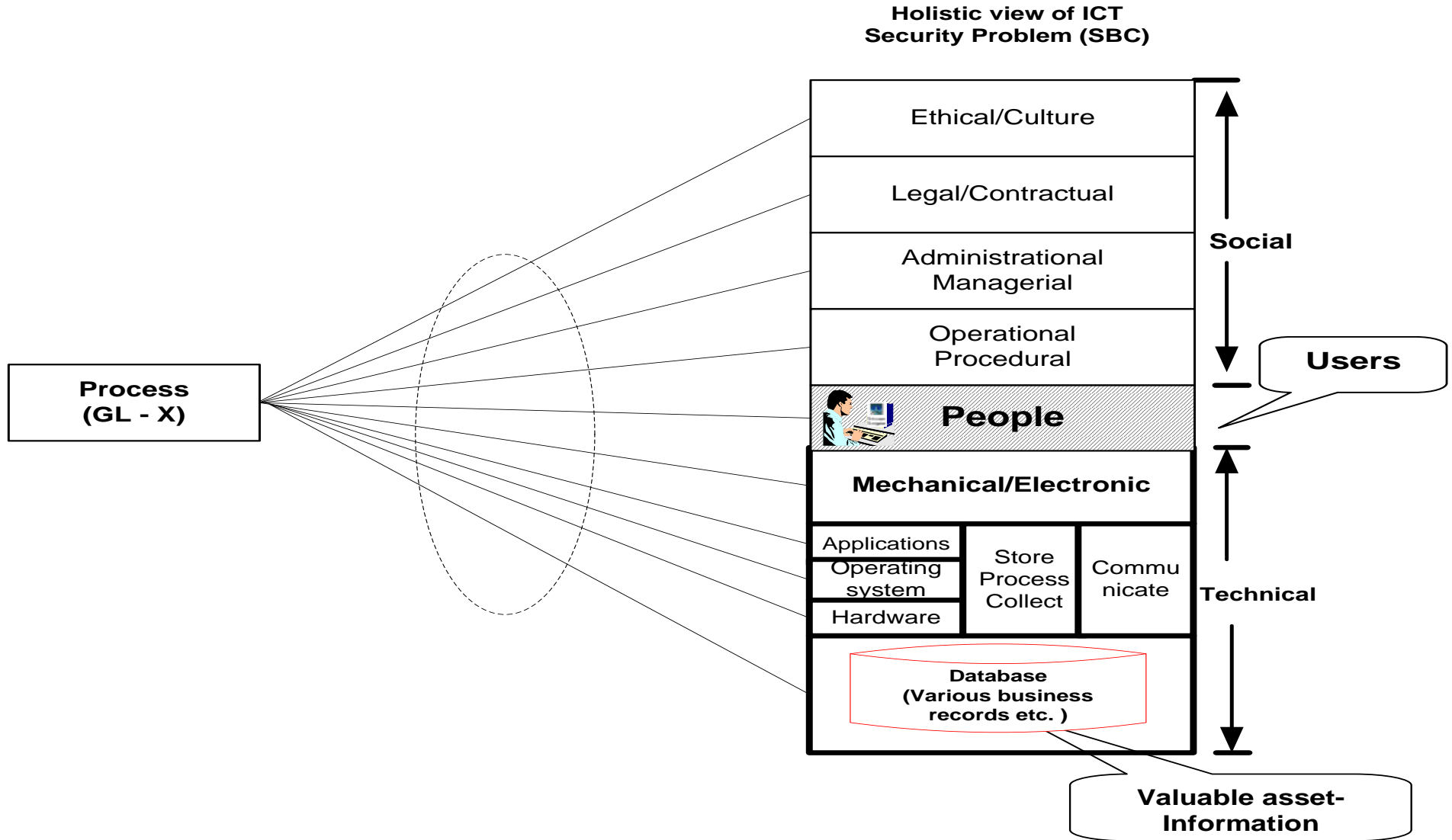
The Environment

The Organisation



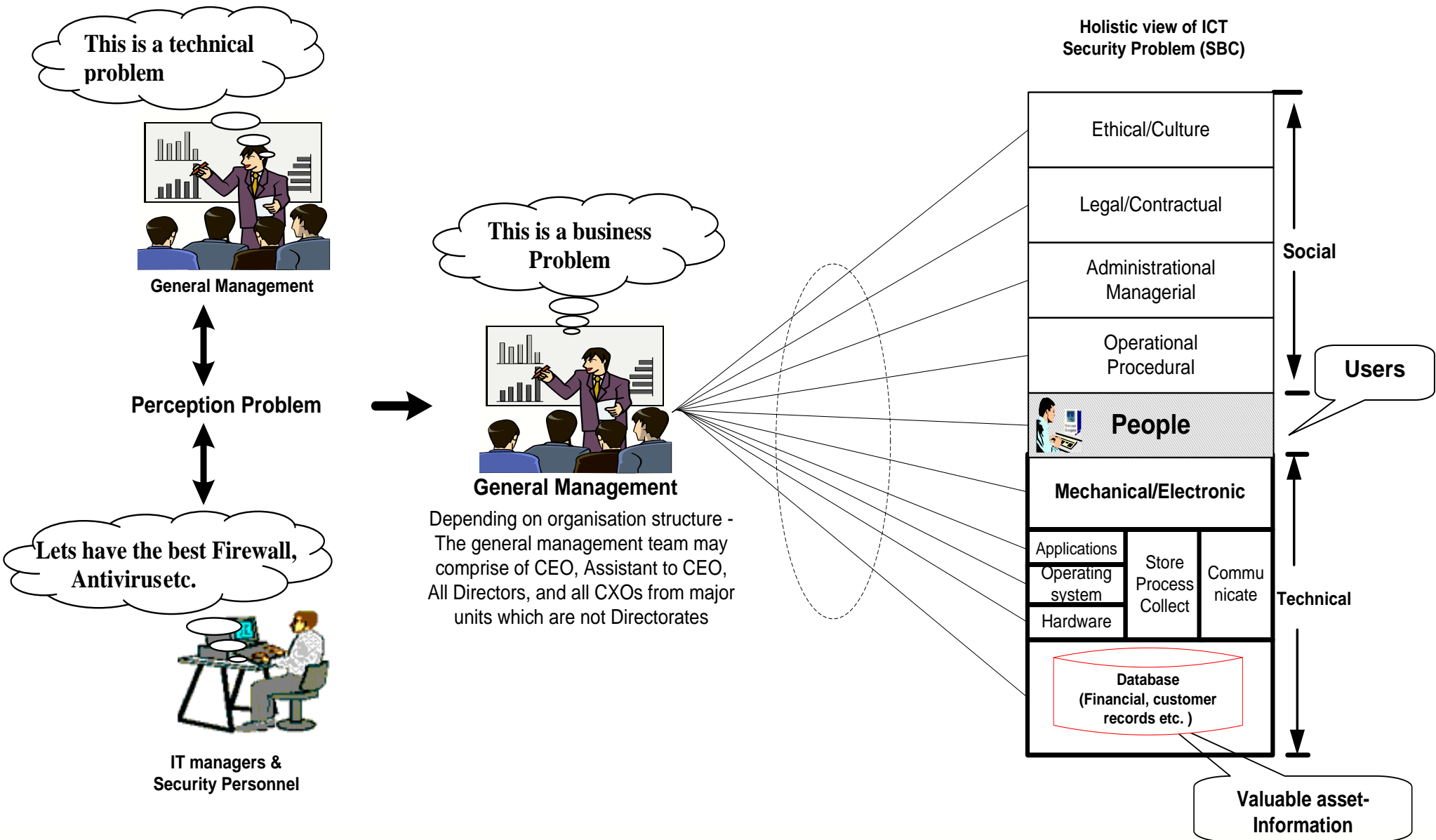


Each process maps the Holistic View of the security challenge





A holistic approach for managing ICT security is required for public-oriented e-Government facilities to be secure!





END

Thank You for Listening