

ISACA Jeddah Chapter Technical Session 7 December, 2010

Information Security Governance

By

Presented by: Ahmed Mirza
President-
ISACA Jeddah Chapter



Information Security Challenges

How to practically use InfoSec as business enabler?

- Perception of InfoSec is that it “creates barriers in business”

How to think of InfoSec at the very beginning of any project?

- Security is always an afterthought

How money spent on InfoSec becomes investment?

- Compliance is looked upon as an additional cost

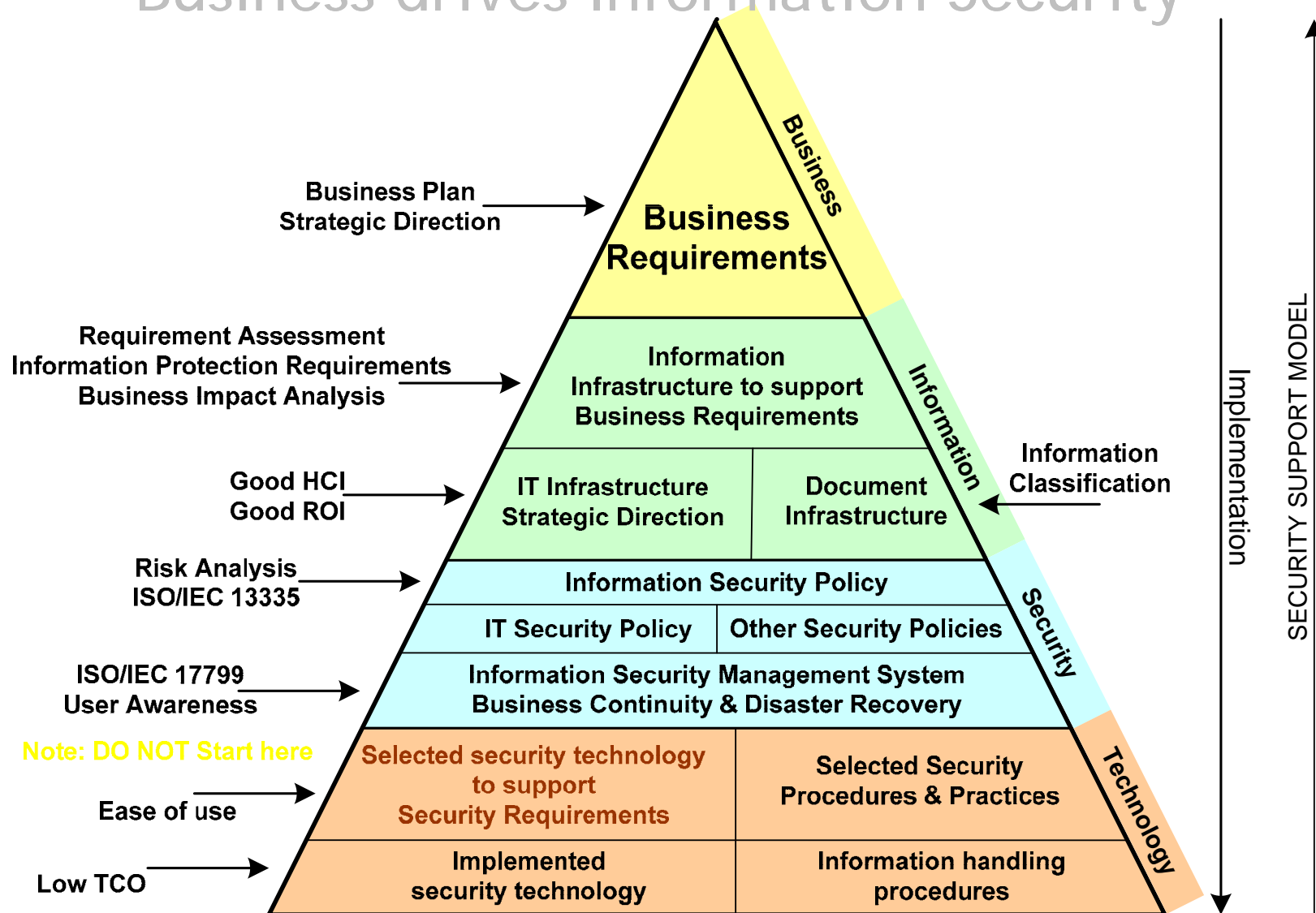
How to have all stakeholders work as a team?

- Business, IT, Comms, InfoSec department

How to migrate to a preventive culture?

- Lack of preventive culture, everywhere in society

Business drives Information Security



What is Information Security Management?

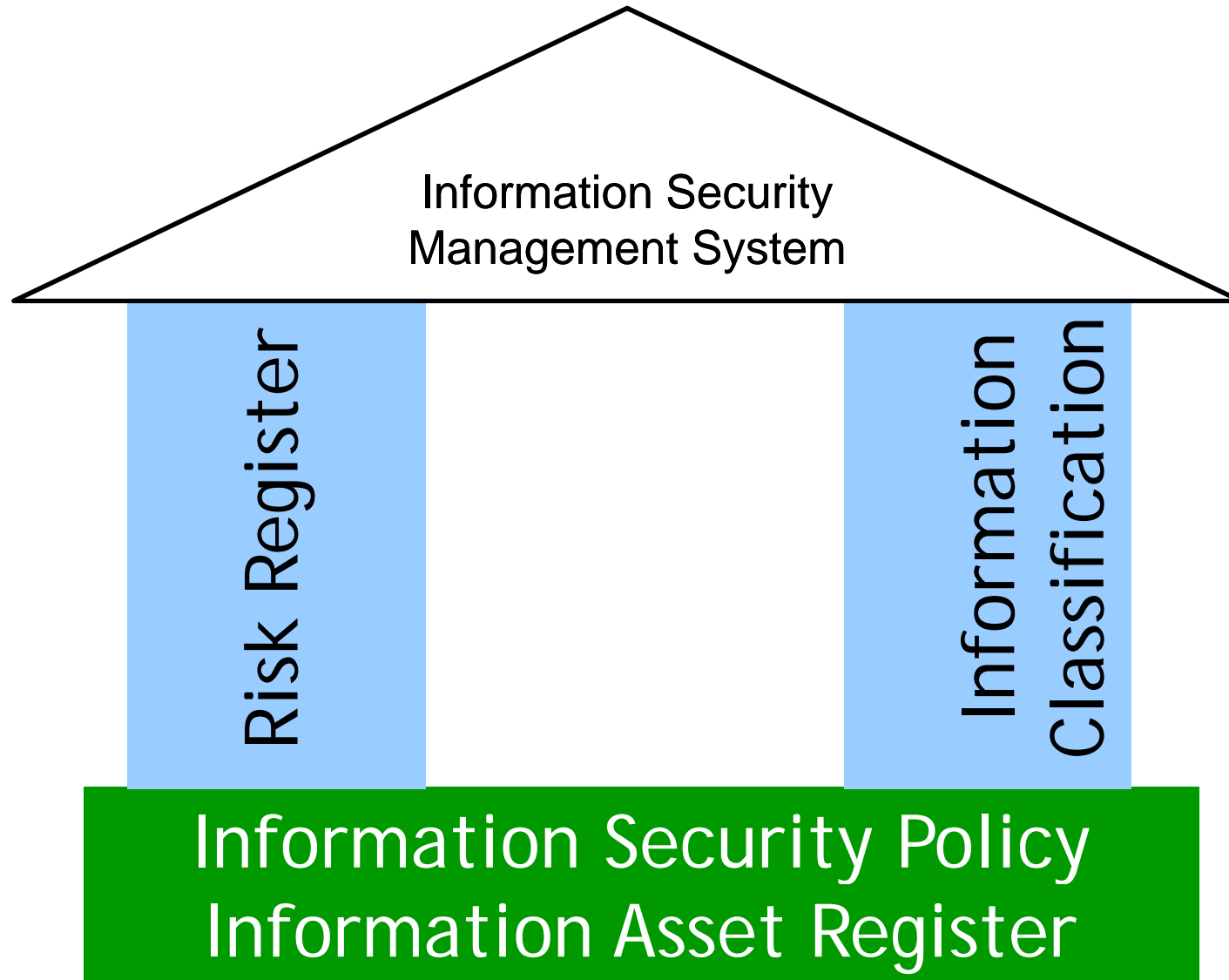


Information Security Management

- ❑ Objective is not to eliminate risk, rather bring it to an acceptable level

- ❑ Managing Risks to Information Assets, on an acceptable level.
 - Know risks impacting Information Assets
 - Define level of acceptable Risks
 - Bring Risks to that acceptable level
 - Maintain risks on the acceptable level

Base & Pillars of an ISMS



Information Assets

Identify Information Assets

- Customer Data
- Core Business System
 - Database ABC
 - Log files
 - Excel sheets with marketing department
 - Printed reports
 - Data that is displayed on monitor
- Payment switch
- Call center
- Etc,

Risk Register

□ Risk Assessment of Information Assets

- Identify impact of C I A breaches
- Identify Threats
- Identify Vulnerabilities that may be exploited for a breach
- Identify Likelihood
- Identify acceptable risk (risks may not be eliminated 100%)
- Identify controls to bring risks to acceptable risks

Develop and implement risk treatment plan

How to establish Information Security Governance?

What is I S G ?

Information Security Governance

Developing, Educating, Governing
Implementation of IS Controls (Policies,
Procedures, Standards, Guidelines, Min
requirements, Technologies
Audit & Forensics

What is ISG ?



S y n e r g i z e d I n p u t

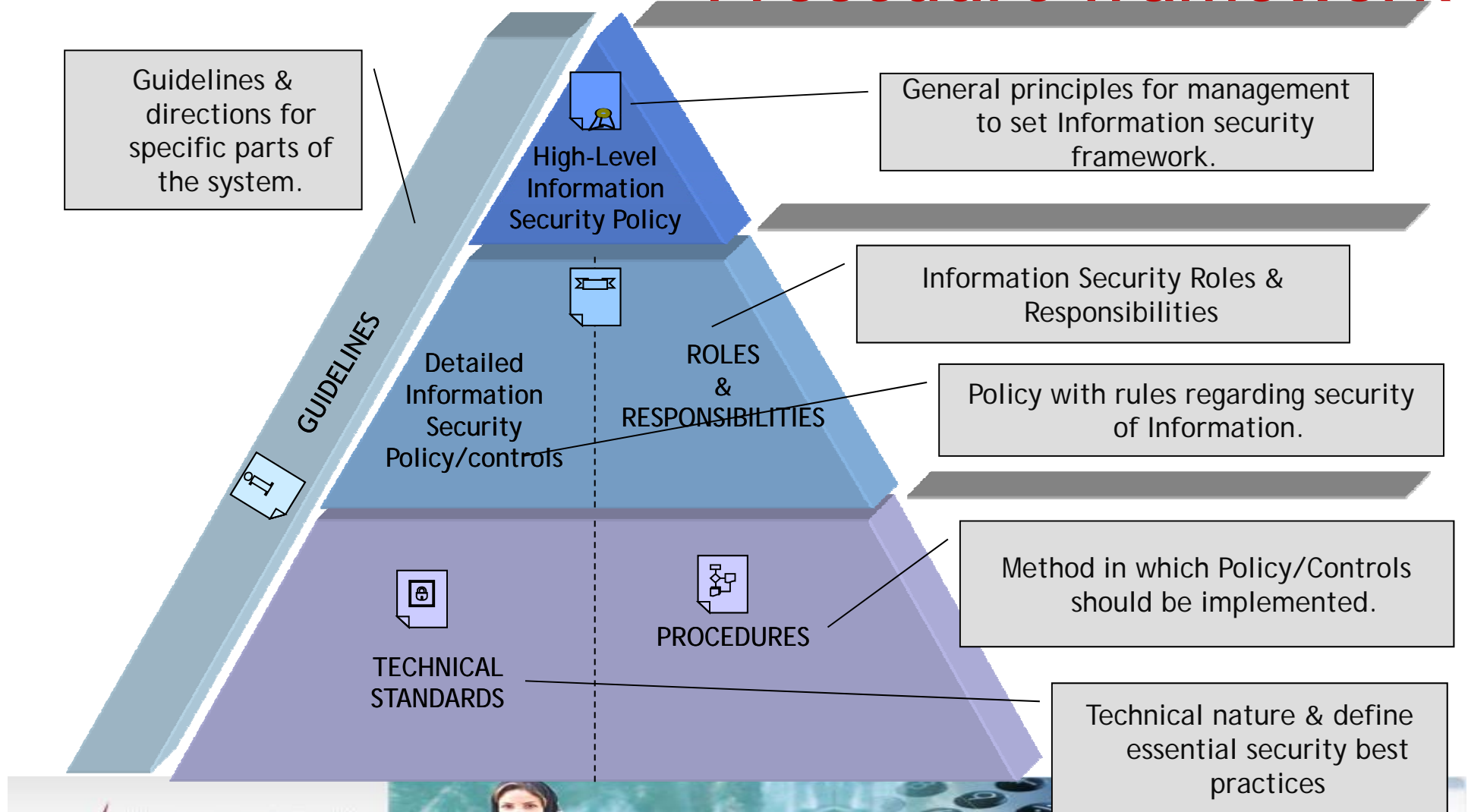
Information Security Governance

Developing, Educating, Governing Implementation of IS Controls (Policies, Procedures, Standards, Guidelines, Min requirements, Technologies)

Audit & Forensics

Risk Mitigation / Risk Treatment Plans

Information Security Policy & Procedure framework



ISG Functions

Governance Decisions for ISMS

Developing ISG framework

Education of IS controls

Governing Implementation

Coordination of implementation

AUDIT (of Information Security Department)

ISG Functions

Governance Decisions for ISMS

Guidance and Approvals on

- ❑ Security Policy, Information Asset & Risk Register
- ❑ IS controls, Risk Treatment plan, Forensics

Audit of IS department

ISG committee / chairman

Developing ISG framework

- ❑ Develop Information Asset Register
- ❑ Develop Risk Register
- ❑ Identify applicable IS controls
- ❑ Develop Risk Treatment plan

Information Security Department



ISG Functions

Education of IS controls

- Policy / Procedures / Standards (selling internally)
- Information Security awareness programs
- L & D of required skills

Competent Security Mgt Team

Governing Implementation

- Development of Framework
- Synergizing & Managing compliance (Regulatory, Best practice)
- Education of IS controls
- Selection of security technologies
- Coordination with relevant departments for implementing controls
- 24x7 security monitoring & CERT
- Audit of controls relevant to other departments

Information Security Department

ISG Functions

Coordination of implementation

- ❑ Single point of contact from each department
- ❑ Participation of all relevant departments
- ❑ Resolving implementation issues & hurdles
- ❑ Input of department wise feedback for continuous update of framework

Information Security Task force

AUDIT (Information Security Department)

Internal Audit or external Consultants reporting to ISG committee

