

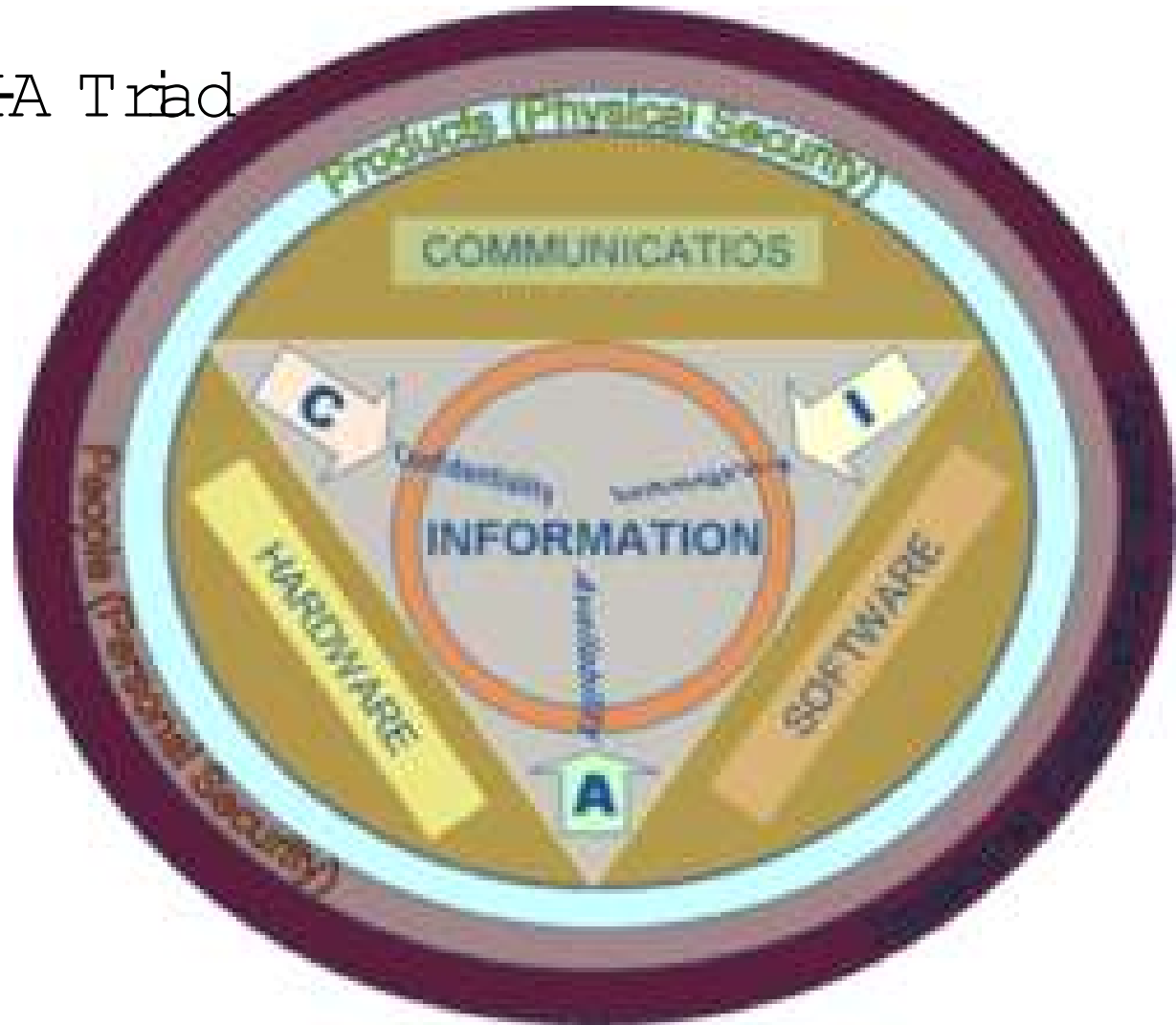


Information Security in Thailand IT industry

Thanat Charoenm ins
19 February 2009

Information Security in Thailand IT industry

C-IA Trad



Information Security in Thailand IT industry

- *Confidentiality* Ensuring that information is accessible only to those authorised to have access.
- *Integrity* Safeguarding the accuracy and completeness of information and processing methods and
- *Availability* Ensuring that authorised users have access to information and associated assets when required.

Information Security in Thailand IT industry

□ Standards

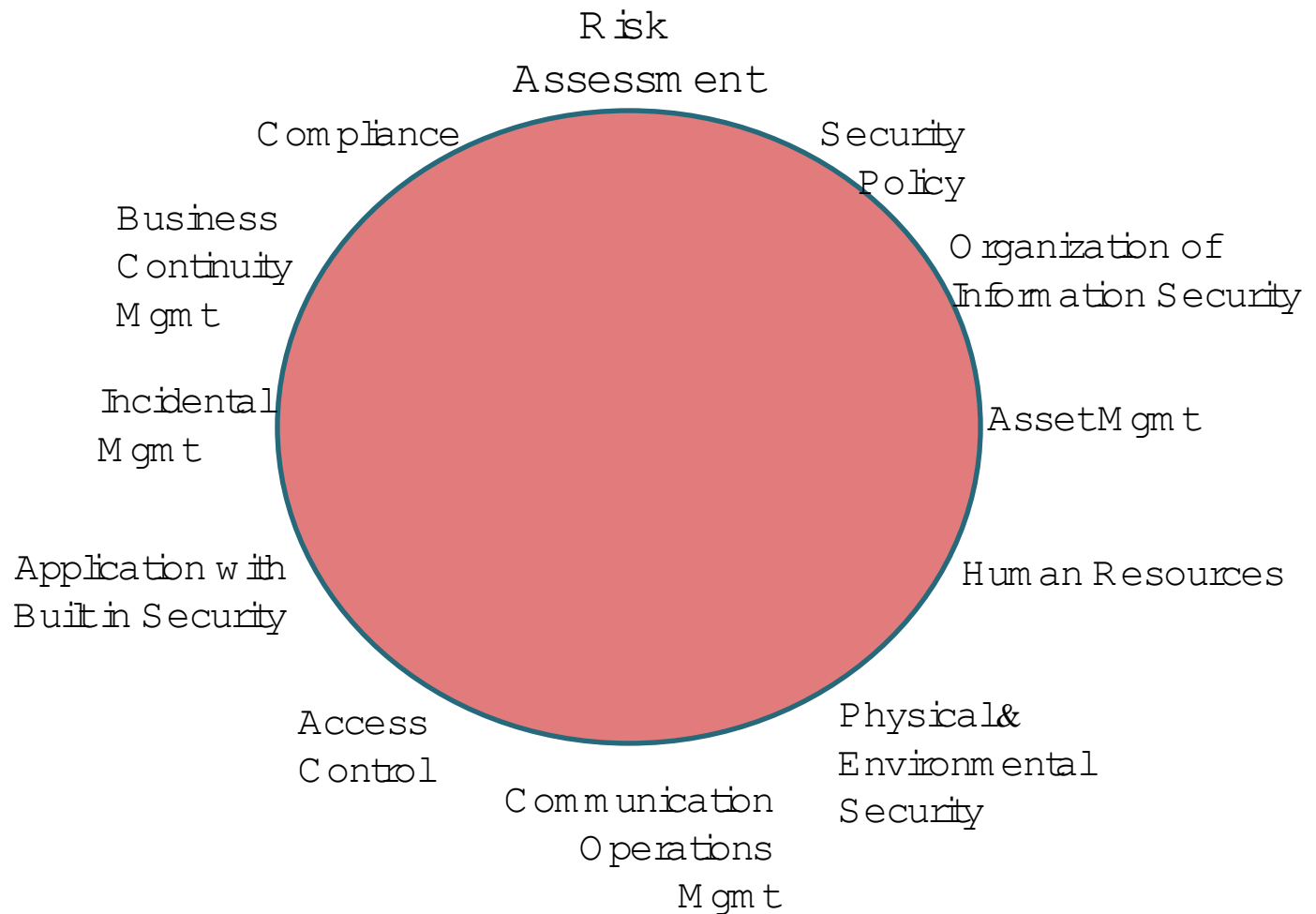
- 'ISO/IEC 27000 series' is an information security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as **ISO/IEC 17799:2005** and subsequently renumbered ISO/IEC 27002:2005 in July 2007, bringing it into line with the other ISO/IEC 27000-series standards.
- ISO/IEC 27002 provides best practice recommendations on information security management.

Information Security in Thailand IT industry

Standard contains :

- Risk Assessment
- Security Policy - management direction
- Organization of information security - governance of information security
- Asset Management - inventory and classification of information assets
- Human resources security - security aspects for employees joining, moving and leaving an organization
- Physical and Environmental Security - protection of the computer facilities
- Communications and operations management - management of technical security controls in systems and networks
- Access Control - restriction of access rights to networks, systems, applications, functions and data
- Information Systems acquisition, development and maintenance - building security into applications
- Information security incident management - anticipating and responding appropriately to information security breaches
- Business continuity management - protecting, maintaining and recovering business-critical processes and systems
- Compliance - ensuring conformance with information security policies, standards, laws and regulations

Information Security in Thailand IT industry



Information Security in Thailand IT industry

□ Security

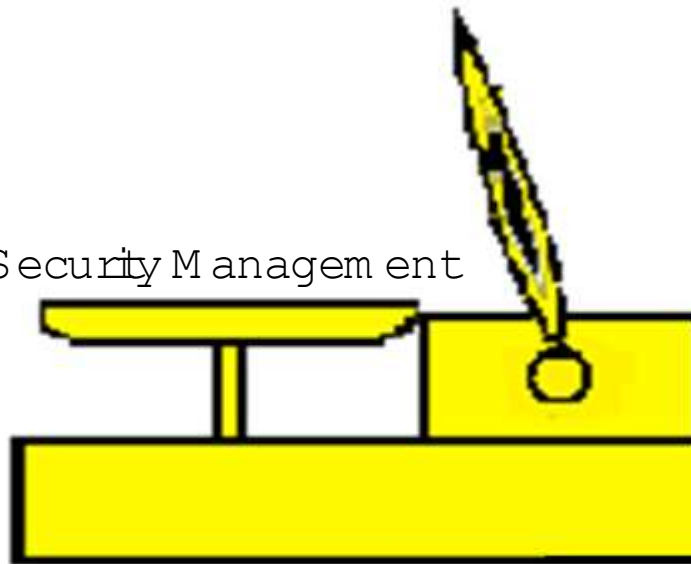
- An insurance policy. The more coverage provided, the higher the premium has to be paid.
- Always been viewed as cost contributor
- An ongoing and repetitive process that must have continuity unended.

Information Security in Thailand IT industry

Least Exposure - Organization Risk - Most Exposure



Security Management



Information Security in Thailand IT industry

- Commonly Found Incidents on
 - Awareness about Security
 - Management commitment to enforce security
 - Monitor & Control
 - Budget
 - Licensing
 - Overpower authority

Information Security in Thailand IT industry

□ Current Situation

- Confidentiality – Low emphasis in Thailand IT industry.
 - Information are not always accessible by authorized personnel only
- Integrity – Medium emphasis
 - Misclassified Information
- Availability - High emphasis
 - 24 x 7 requirement due to service nature
 - DRCs

Information Security in Thailand IT industry

▣ Visible Leak

- Premises
- Access Control
- Falsely classified resources

▣ Invisible Leak

- Unsecure wireless network linkage
- Procedural
- Authority
- Unaware of classified ad

Information Security in Thailand IT industry

□ Some Statistics

- **94%** of IT users know and recognize the importance of security matters, only **53%** practice them .
- **31%** of organization employees allow unknown visitors to enter restricted area .
- **43%** of changed position employees still have access to the security assets of their previous position .