

Welcome to presentation  
by



NETPECKERS CONSULTING (P) LTD.

**An ISO 9001:2000 compliant organization**

*Sanjay Punjabi*

*Lead Auditor ISO 9001:2000, ISO 14001:2004,  
OHSAS 18001:1999, BS-7799, ISO 22000:2005,  
ISO 27001:2005*

On

**Direct & Indirect Advantages of implementing  
ISO 27001:2005 in your organization**



DURATION 25 MINUTES.

## What Is ISO 27001?

- ISO 27001, titled "Information Security Management - Specification With Guidance for Use", is the replacement for BS7799-2. It is intended to provide the foundation for third party audit, and is 'harmonized' with other management standards, such as ISO 9001 and ISO 14001.

## Objective of the standard

- The basic objective of the standard is to help establish and maintain an effective information management system, using a continual improvement approach. It implements OECD (Organization for Economic Cooperation and Development) principles, governing security of information and network systems.

# The Contents of the Standard?

- The broad content is of course similar to the old BS7799. Included is:
- Cross reference with ISO 17799 controls
- Use of PDCA
- Information Management System
- Terms and definitions

## 1) When was ISO 27001 published?

- In October 2005, although a final draft version was published some months prior to this.

## 2) Is it related to ISO 17799?

- Yes. It essentially described how to apply the controls defined within ISO 17799, and of course how to build and maintain an ISMS.



# **ISMS – INFORMATION SECURITY MANAGEMENT SYSTEM**

# Types of Information

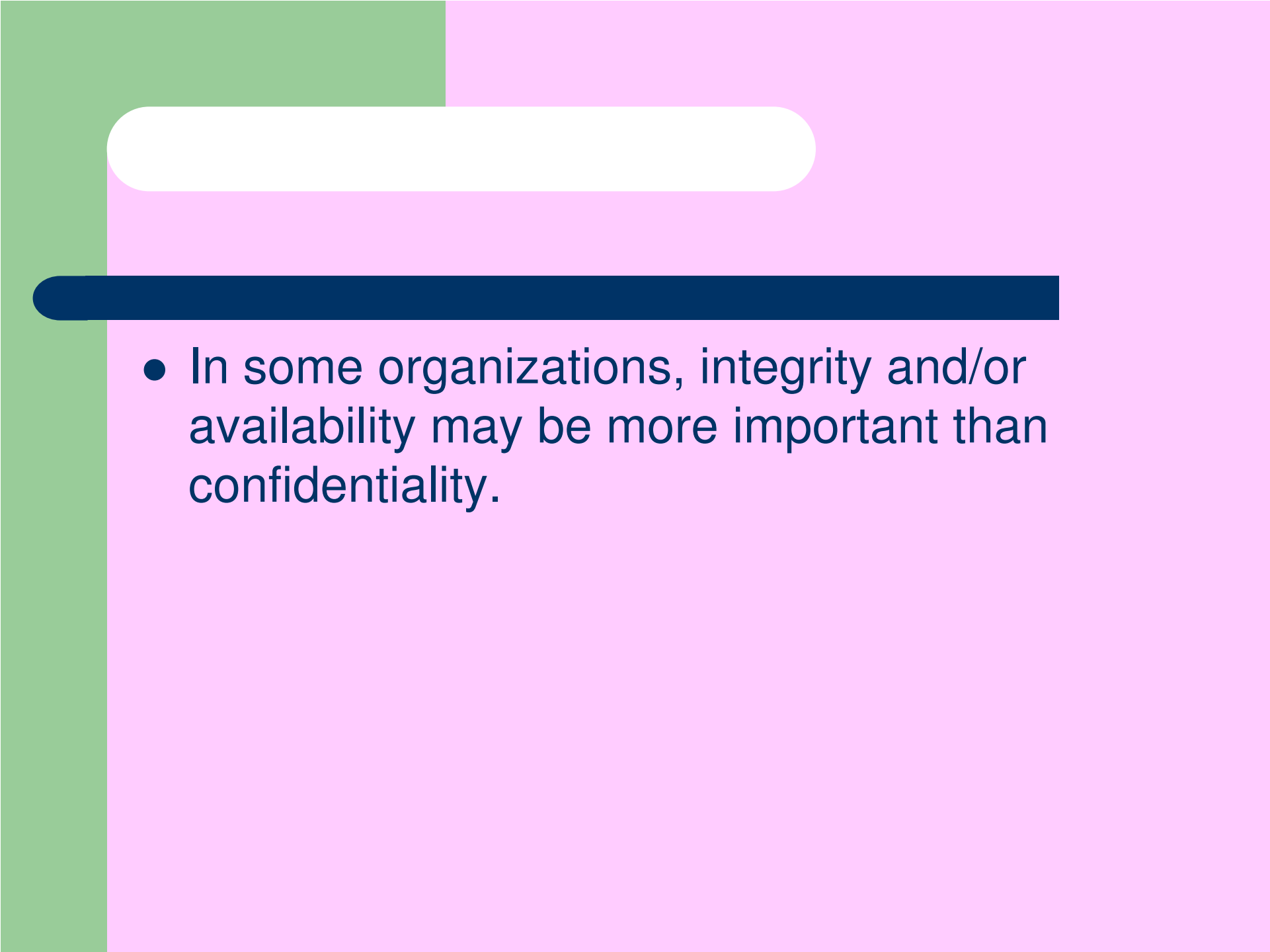
- Printed or written on paper
- Stored electronically
- Transmitted by post or using electronic means
- Shown on corporate videos
- Verbal-spoken in conversations

*'...Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected'(ISO 17799:2005)*

# What is Information Security

ISO 27001:2005 defines this as:

- **Confidentiality** : the property that information is not made available or disclosed to unauthorized individuals, entities(programs), or processes (superceding processes)
- **Integrity** : the property of safeguarding the accuracy and completeness of assets.
- **Availability** : the property of being accessible and usable upon demand by an authorized entity.

- 
- In some organizations, integrity and/or availability may be more important than confidentiality.

# Role of ISMS

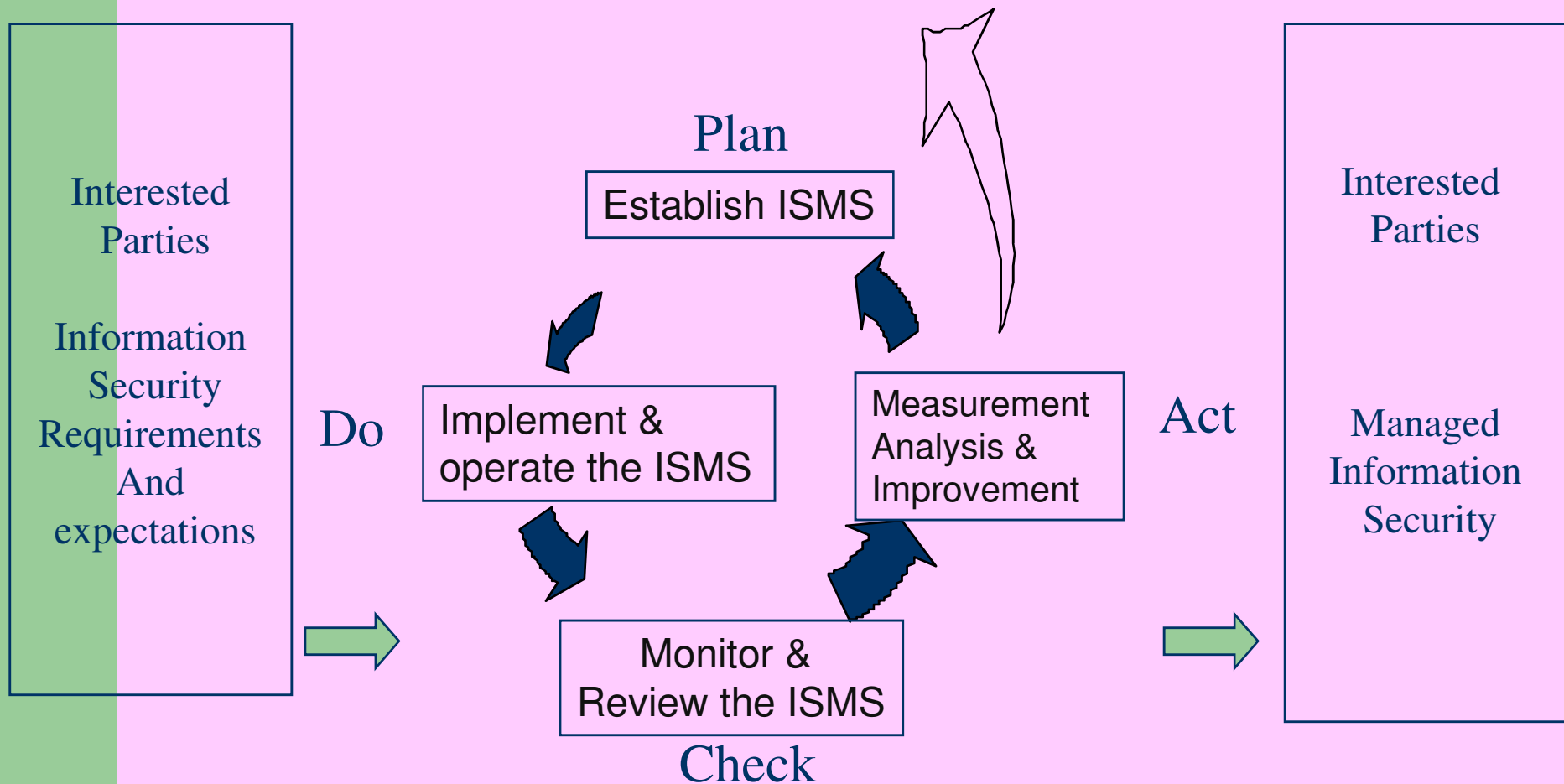
- Information security protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investment and business opportunities.
- Every organization will have a differing set of requirements in terms of control requirements and the level of confidentiality, integrity and availability.

# Eight Management Principles

1. Customer focus
2. Leadership
3. Involvement of people
4. Process approach
5. System approach to management
6. Continual improvement
7. Factual approach to decision making
8. Mutually beneficial supplier relationship.

# Management Process Model

Continual Improvement of the Management System



# Risks and Threats to Information Systems

- High User knowledge of IT system.
- Theft, Sabotage, Misuse, Hacking.
- Version control problems.
- Unrestricted access.
- Systems/ network failure
- Lack of documentation
- Virus
- Natural calamities
- Fire

# Information Security – General trends

- 20% of large organizations that had an incident took more than a week to get business operations back to normal.
- “Virus infection was the single largest cause of serious security breaches.”
- 44% of UK business have suffered at least one malicious security breach in the year 2001. Average cost of a serious security incident was £30,000.
- “Only 27% UK companies have documented security policy.”
- “Only 33% of UK web-site have software in place to detect intrusion.”

INFORMATION SECURITY BREACHES SURVEY 2002

# Information Security – General trends contd...

## ❖ Issues at a glance

- Ninety percent of organizations say information security is of high importance for achieving their overall objectives.
- Seventy-eight percent of organizations identify risk reduction as their top influence for information security spending.

Source: Global Information Security Survey 2003 by Ernst & Young.

# Information Security- General trends contd...

- However
  - More than 34% of organizations rate themselves as less than adequate in their ability to determine whether their systems are currently under attack.
  - More than 33% of organizations say they are inadequate in their ability to respond to incidents.
  - Only 34% of organizations claim to be compliant with applicable security –driven regulations.
  - Fifty six percent of organizations cite insufficient budget as the number one obstacle to an effective information security posture.
  - Nearly 60% of organizations say they rarely or never calculate ROI for information security spending.
  - Only 29% of organizations list employee awareness and training as a top area of information security spending, compared with 83% of organizations that list technology as their top information security spending area.
  - Only 35% of organizations say they have continuous education and awareness programs.

Source: Global Information Security Survey 2003 by Ernst & Young.

# Result ?????

- Uncertainty over issues such as
  - Availability
    - Is information accessible wherever and whenever required?
  - Integrity
    - Is information sufficiently right for the purpose at the time of use?
  - Confidentiality
    - Is information available only to those who are authorised to access IT?

***This is likely to result in lower trust levels.***

# And the Challenge is ...

Protection of Information and Information Systems to meet Business and Legal Requirement by

- Provision and demonstration of secure environment to clients.
- Managing security between projects from competing clients
- Preventing loss of product knowledge to external attacks, Internal thefts
- Preventing Leak of confidential information to competition.
- Meeting Parent company requirements
- Ease of access to large mobile work force.
- Providing access to customers where off site development is undertaken with the client.
- Introduction of new technologies and tools
- Managing costs Vs risk
- Managing Legal compliance.

**Thank you for joining in the presentation  
Please fill in the feedback form  
Which would help us to be more precise  
In our efforts.**

**Sanjay Punjabi  
Certified Auditor  
[san@netpeckers.net](mailto:san@netpeckers.net)  
M-9426077684**



An ISO 9001:2000 compliant organization

