ISMS Excerpts – General Overview

WHAT IS INFORMATION?

- Information is an asset which like other important business assets, has value to an organization and consequently needs to be suitably protected

"Information Security is Everyone's Responsibility"

INFORMATION TYPES

- Information exists in many forms:
  - Printed or written on paper
  - Stored electronically
  - Transmitted by post or electronic means
  - Visual e.g. videos, diagrams
  - Published on the Web
  - Verbal/aural e.g. conversations, phone calls
  - Intangible e.g. knowledge, experience, expertise, ideas

"Information Security is Everyone's Responsibility"

INFORMATION LIFECYCLE

- Information can be …
  - Created
  - Owned (it is an asset)
  - Stored
  - Processed
  - Transmitted/communicated

"Information Security is Everyone's Responsibility"

INFORMATION LIFECYCLE

- Used (for proper or improper purposes)
- Modified or corrupted
- Shared or disclosed (whether appropriately or not)
- Destroyed or lost
- Stolen
- Controlled, secured and protected throughout its existence

"Information Security is Everyone's Responsibility"

WHAT IS INFORMATION SECURITY?

- Information security is what keeps valuable information 'free of danger' (protected, safe from harm)
- 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)

"Information Security is Everyone's Responsibility"

WHAT IS INFORMATION SECURITY?

- Protecting CIA (Confidentiality, Integrity and Availability)
- Avoiding, preventing, detecting and recovering from incidents
- Securing people, processes and technology … not just IT!

"Information Security is Everyone's Responsibility"

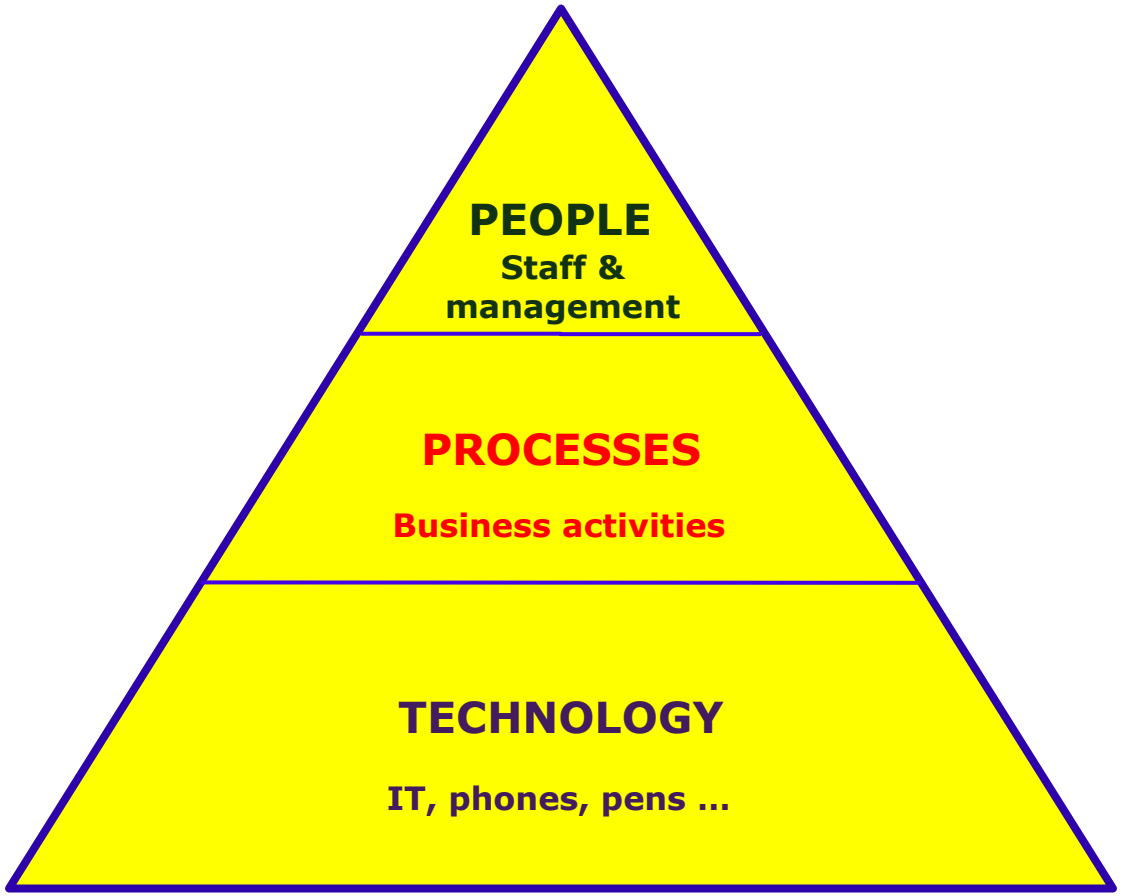
ESSENTIAL ATTRIBUTES OF SECURITY

- Information security is defined as the preservation of:

Confidentiality	Making information accessible only to those authorized to use it
Integrity	Safeguarding the accuracy and completeness of information and processing methods
Availability	Ensuring that information is available when required

"Information Security is Everyone's Responsibility"

SECURITY ELEMENTS



"Information Security is Everyone's Responsibility"

PEOPLE

- People who use or have an interest in our information security include:
  - Shareholders / owners
  - Management & staff
  - Customers / clients, suppliers & business partners
  - Service providers, contractors, consultants & advisors
  - Authorities, regulators & judges

- Our biggest threats arise from people (social engineers, unethical competitors, hackers, fraudsters, careless workers, bugs, flaws …), yet our biggest asset is our people (e.g. security-aware employees who spot trouble early)

"Information Security is Everyone's Responsibility"

PROCESS

- Processes are work practices or workflows, the steps or activities needed to accomplish business objectives
  - Processes are described in procedures
  - Virtually all business processes involve and/or depend on information making information a critical business asset

- Information security policies and procedures define how we secure information appropriately and repeatedly

"Information Security is Everyone's Responsibility"

TECHNOLOGY

- Information technologies
- Cabling, data/voice networks and equipment
- Telecommunications services (PABX, VoIP, ISDN, videoconferencing)
- Phones, cell phones, PDAs
- Computer servers, desktops and associated data storage devices (disks, tapes)
- Operating system and application software
- Paperwork, files
- Pens, ink
- Security technologies
- Locks, barriers, card-access systems, CCTV

"Information Security is Everyone's Responsibility"

VALUES

- Protects information against various threats
- Ensures business continuity
- Minimizes financial losses and other impacts
- Optimizes return on investments
- Creates opportunities to do business safely
- Maintains privacy and compliance

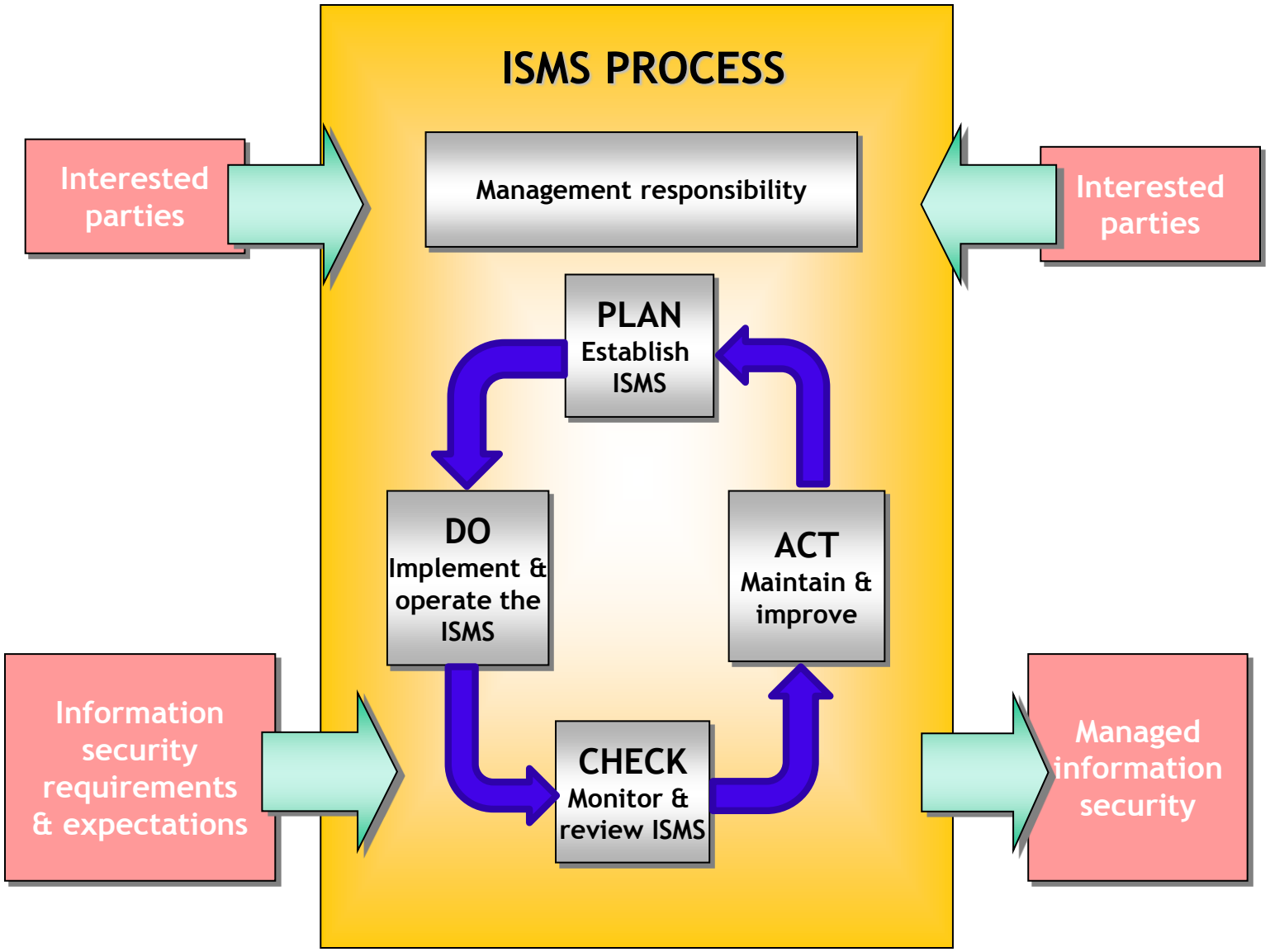
"Information Security is Everyone's Responsibility"

INTRODUCTION TO ISO27K

- 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
- It protects the employees identity by defining clear rules and methods for authentication, and for protection of identity data - therefore, the chance that someone's identity is going to be misused is much lower.

"Information Security is Everyone's Responsibility"

PDCA CYCLE FOR ISMS IMPLEMENTATION



"Information Security is Everyone's Responsibility"

INFORMATION SECURITY METRICS

Information Security Metrics

Aspire Systems has defined the information security metrics for mainstreams and support services.

Following, Information security metrics for development and testing was introduced

a. % of Ontime Removal of Access

b. % of Ontime Return of Assets

c. Security Defect Leakage

This can be found in the Metrics Analysis Plan

Security requirements for the applications can be found in Non-Functional Requirement document. If required, this can be monitored as new metric for the project.

"Information Security is Everyone's Responsibility"

INFORMATION SECURITY POLICY STATEMENT

Information Security Policy Statement

Aspire Systems is a global technology services firm serving as a trusted technology partner for its customers. Aspire Systems focuses on four service operations that include Product Engineering, Independent Testing services, Enterprise Transformation and Infrastructure Application Support.

Information Technology being the key driver for Aspire services to its customers, the management recognizes Information and related technology as a strategic business asset of significant value to the company and its customers that needs to be diligently protected.

"Information Security is Everyone's Responsibility"

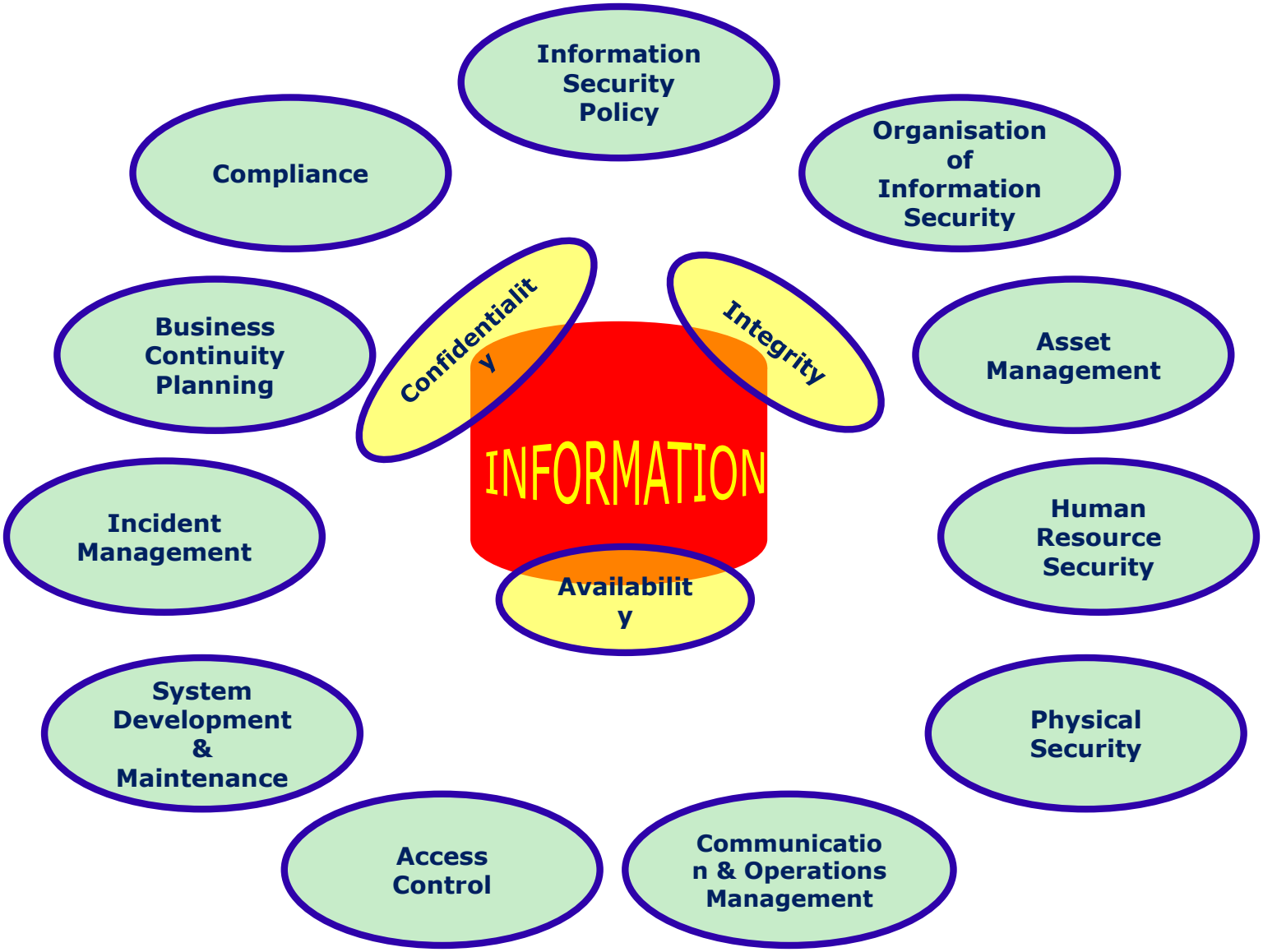
INFORMATION SECURITY POLICY STATEMENT (CONT)

To achieve the above, Aspire shall:

- Establish and implement policies, processes and organization structures (Information Security Management System) to protect the information assets of Aspire and its customers from threats, both external as well as internal.
- Continually improve the Information Security Management System by adopting a life cycle approach through the establishment and regular monitoring of measurable security objectives.
- Commit to comply with business, legal, regulatory and contractual security obligations, as may be applicable from time to time.
- Ensure confidentiality, integrity and availability of the information assets of its customers and other stakeholders.
- Develop, implement test and maintain a Business Continuity Plan.
- Create mechanisms to identify and review the risk and impact of breaches in protected information assets
- Communicate all pertinent security policies to employees, customers and other interested parties as applicable.
- This policy applies to all employees of Aspire and other users of Aspire's information processing facilities. The CEO and the senior management shall ensure that this policy is implemented, communicated, monitored and maintained at all levels of the organization and regularly reviewed for compliance and continual improvement.

"Information Security is Everyone's Responsibility"

CONTROL CLAUSES



"Information Security is Everyone's Responsibility"

CONTROL CLAUSES

- **Information security policy** - management direction
- **Organization of information security** - management framework for implementation
- **Asset management** – assessment, classification and protection of valuable information assets
- **HR security** – security for joiners, movers and leavers
- **Physical & environmental security** - prevents unauthorized access, theft, compromise, damage to information and computing facilities, power cuts
- **Communications & operations management** - ensures the correct and secure operation of IT

"Information Security is Everyone's Responsibility"

CONTROL CLAUSES

- **Access control** – restrict unauthorized access to information assets
- **Information systems acquisition, development & maintenance** – build security into systems
- **Information security incident management** – deal sensibly with security incidents that arise
- **Business continuity management** – maintain essential business processes and restore any that fail
- **Compliance** - avoid breaching laws, regulations, policies and other security obligations

"Information Security is Everyone's Responsibility"

BENEFITS

- Demonstrable commitment to security by the organization
- Legal and regulatory compliance
- Better risk management
- Commercial credibility, confidence, and assurance
- Reduced costs
- Clear employee direction and improved awareness

"Information Security is Everyone's Responsibility"

CHANGE MANAGEMENT

- Any changes in the system to be approved by CCB (Change Control Board)
- The Changes are analyzed, tested before implementation
- The primary goal of the Change management process is to accomplish changes with minimum
  - Business Impact
  - Cost
  - Risk

"Information Security is Everyone's Responsibility"

WHO IS RESPONSIBLE

- Information Security Management Committee
- Information Security Manager/CISO (Chief Information Security Officer) and Department
- Incident Response Team
- Business Continuity Team
- IT, Legal/Compliance, HR, Risk and other departments
- Audit Committee
- Last but not least, **you**!
  - Note – The detailed Roles and Responsibilities can be found in Q:\Process\Documents\ISMS\R and R
- *Information security awareness training or program is meant for*

  Employees, Contractors, Vendors

"Information Security is Everyone's Responsibility"

ISO 27001 ROAD MAP

- Creating INFORMATION SECURITY AWARENESS
- Performing RISK ASSESSMENT
- Performing a Gap analysis
- Drafting ISMS policies, procedures
- Training the organisation at different levels for the relevant ISMS areas
- Creating a Business Continuity and Disaster recovery Plan and testing
- Performing Internal Audits on the systems readiness
- Closing the findings of the Internal audits on ISMS
- Undergoing an external Certification Audit
- Closing findings of the certification Audit
- Getting certified to ISO 27001
- Continual governance of the ISMS system

"Information Security is Everyone's Responsibility"

THANK YOU

"Information Security is Everyone's Responsibility"

aspire SYSTEMS
attention. always.