

e-City as an e-Government Approach:

IT Service and Information Security Management Systems

Based on

BS7799 and BS15000

Houman Sadeghi Kaji

Spread Spectrum Communication System PhD. ,

Cisco Certified Network Professional Security Specialist

BS7799 LA

info@houmankaji.net



Topics:

- ***e-Government and e-City***
- **Key Challenges in the Transformation to e-City as an e-Government**
- **BS7799 – Information Security Management System**

مید رساند ای

نخستین



e-Government and e-City: Terms and Definition

What is e-Government?



Information
available
online

Two-way
communication

Transaction
handled
online

Process,
system and
organisational
integration

Entirely new
services
delivered cross-
agency through
a centralised
enterprise portal

The application of ICT in interactions between

- Government and Citizens
- Government and Businesses
- Government and Employees
- Government and Government

to simplify and improve democratic, government and business aspects of Governance.



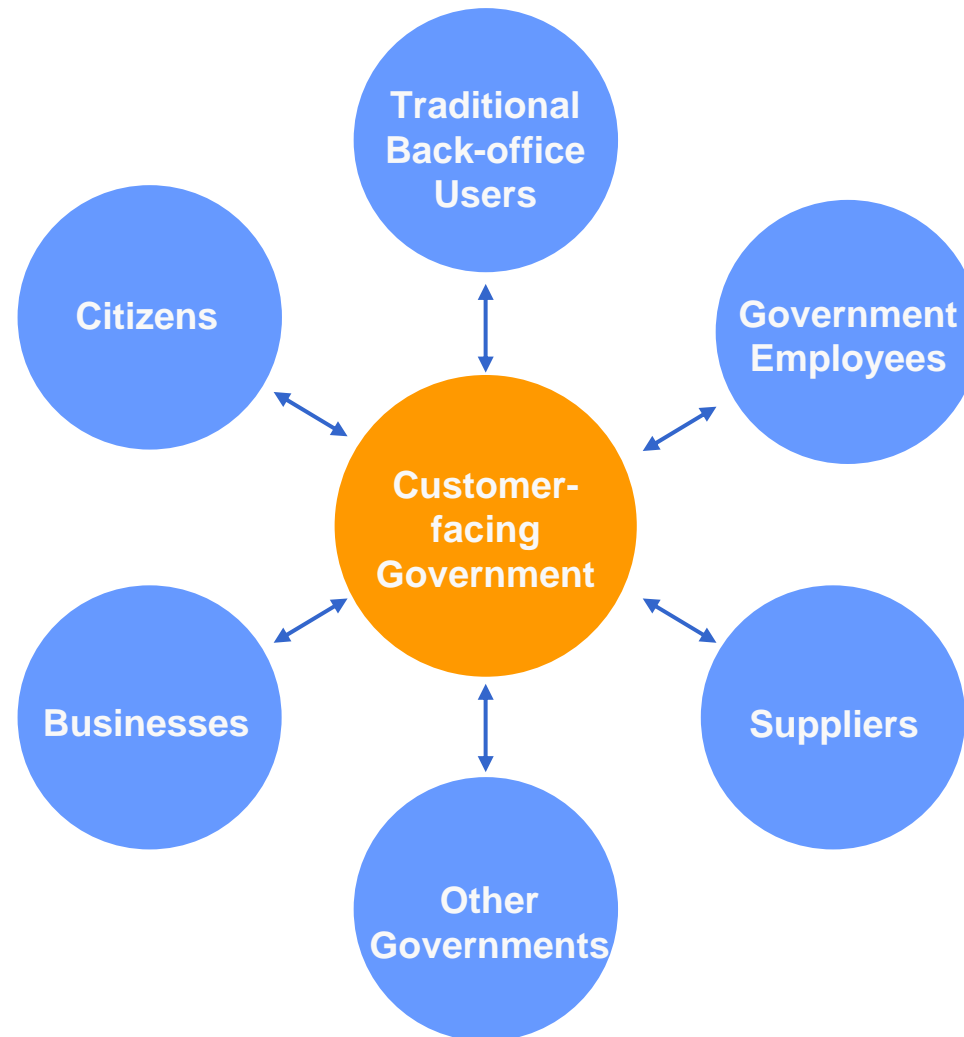
A Revolution in Rising Expectations



هدایت و توسعه
وزارت ارتباطات و فناوری اطلاعات

- Citizens want the ease and convenience of 24x7 access and one-stop services
- Businesses want same level of service as in the private sector
- Governments recognize the opportunity to
 - Provide new means of access to government services
 - Introduce self-service models
 - Deliver personalized government services, tailored to the needs of stakeholder groups

Customer-facing Government Touches All Stakeholders



Characteristics of Successful e-Governmetn



- Customer Access — Offer **personalized access** to services, 7x24
- High Value Transactions — Use technology to **increase the efficiency and effectiveness of transactions** with citizens, suppliers, and other stakeholders
- Customer Relationships — Implement solutions that enable governments to effectively **manage relationships** with their constituencies
- End-to-End Intelligence — Implement solutions that deliver **end-to-end intelligence through enterprise-wide integration**

Characteristics of Successful e-Government



- Value chain...understand complete business processes, and automate the workflow and linkages across multiple role performers, to add value at each step
- Single Face of government...present a uniform and standardized user interface, and link related Government functions in a manner optimized for customer convenience
- Self Service...empower the customers to do certain work themselves, improving accuracy and freeing up government resources



Vision



All residence of city regardless of his/her level of education should be able to use electronic services of City Municipality (CM) from any where and any time using the technologies that suites him/her.

Muscat, OMAN

- Create mechanism to **provide information outside** the Municipality premises and working hours
- Provide E services using different type of **technologies**
- Public should be able to **pay electronically** (E-Payment)
- Create **awareness** programs for Municipality Employees and the general public
- Create **new rules** and regulations to suit and supports E-services.
- **Motivate** the public to use E-services



The Terms of *e-City*

The *e-City* is a step of *e-Government* that means the City that protected by **E Services** provided by **Government sectors** same as **Municipality**.



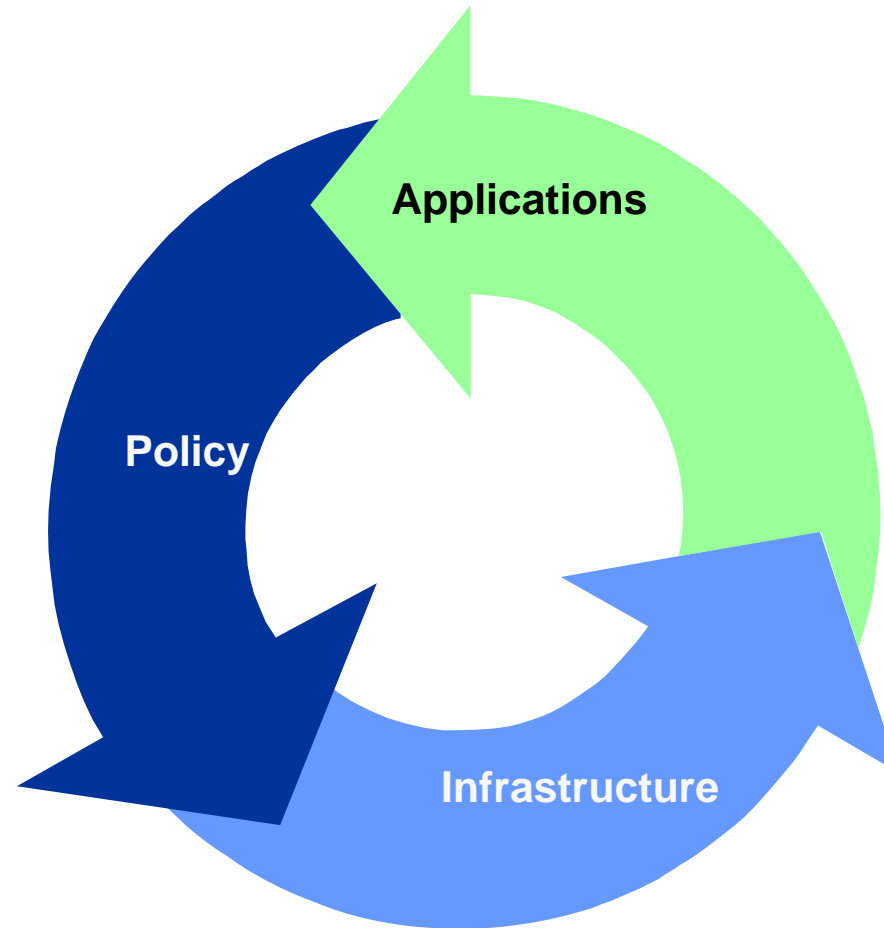
*Key Challenges in the Transformation to
e-City as an e-Government step*

Fundamental Differences Between Municipality and Private Sector

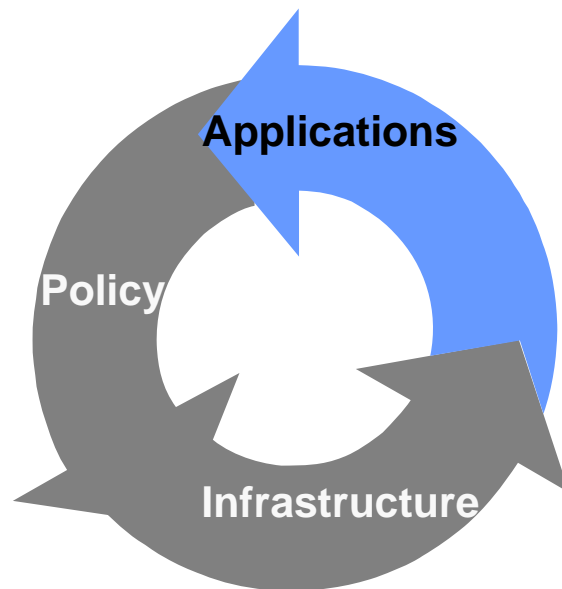


- **Sovereignty** — Municipalities are unique in their sovereign role over citizens
- **Privacy/Security** — privacy and security are directly tied to public trust
- **Responsibility to Serve All** — Municipalities cannot select their “customers”
- **Distribution of value** — Municipalities are subject to different business models
- **Incentives and organization** — checks and balances

Three Interdependent Building Blocks of e-City

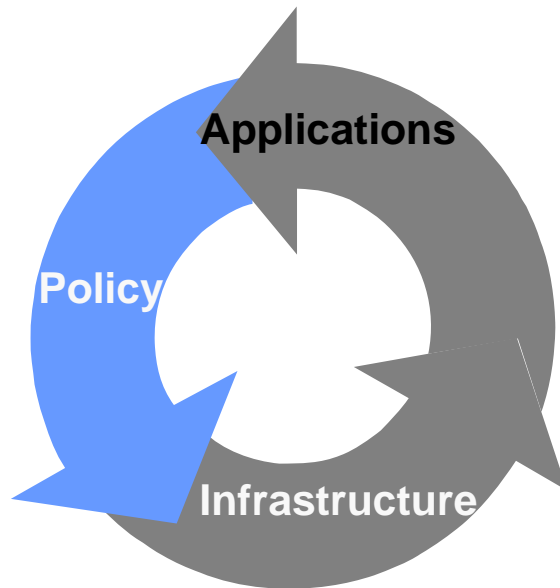


Defining Web-Enabled Applications That ...



- Meet the needs of
 - Citizens
 - Businesses
 - Suppliers
 - Employees
 - Other Municipalities
- Deliver maximum value through integrated end-to-end solutions

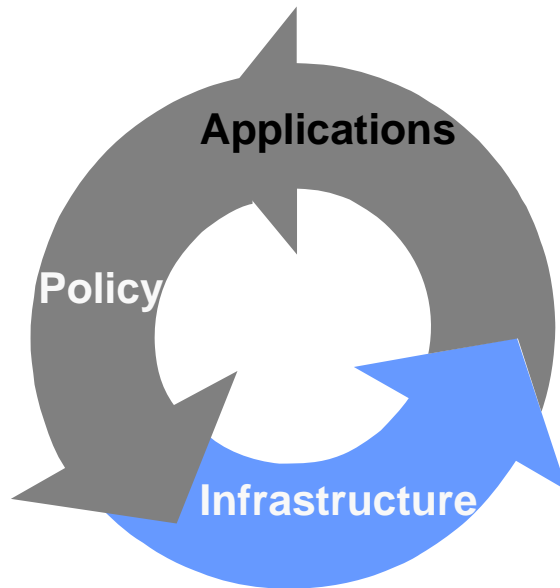
Establishing Policies to Support e-City



Based on shared vision of common enterprise-wide solution

- Data architecture/ownership
- Privacy
- Security
- Standards
- Records management and archiving
- Others...

Creating e-City Infrastructure...

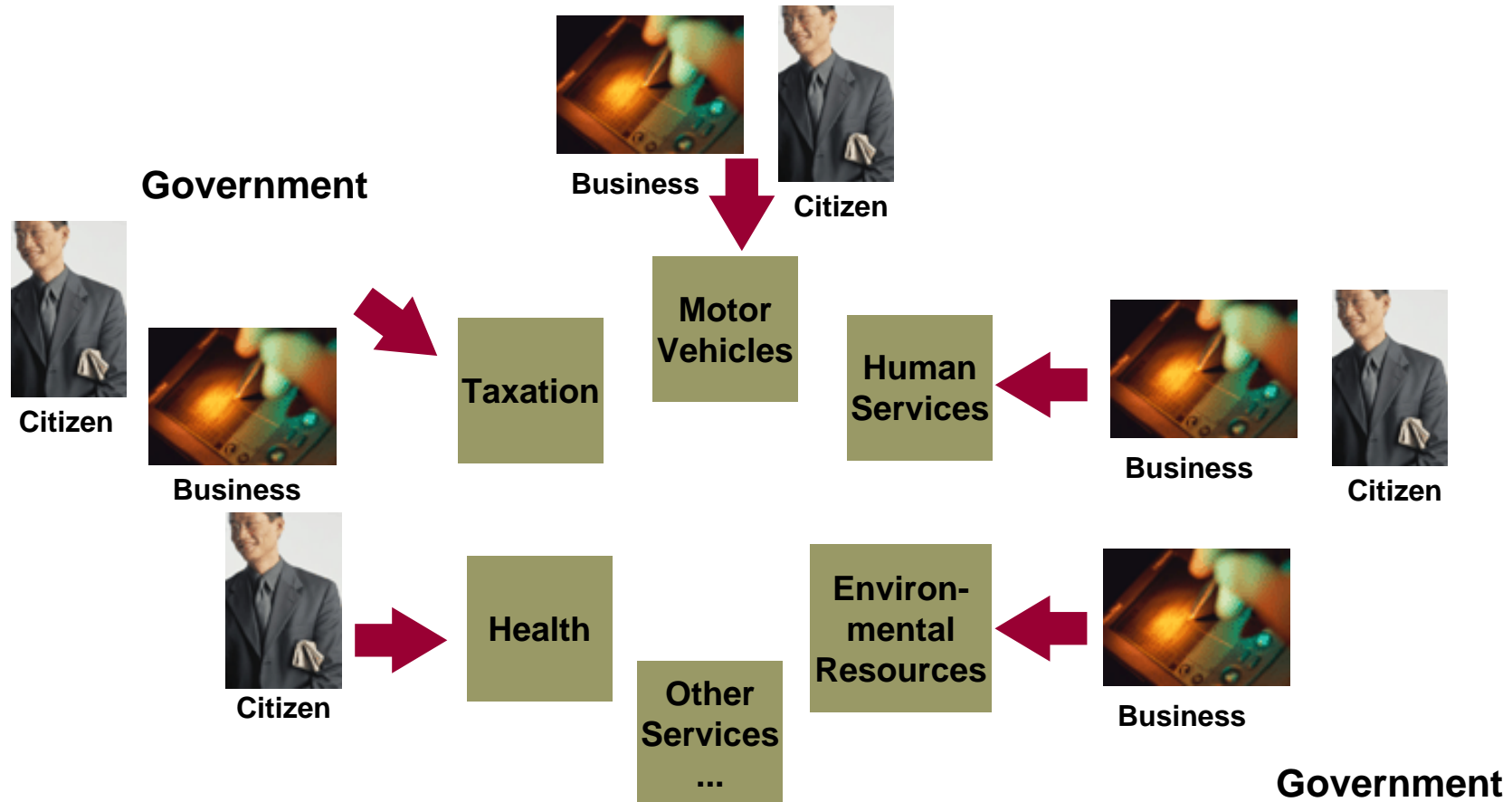


Consisting of...

- Portals
- Enterprise Application Integration
- Security
- Network Capacity
- Electronic Payment Services
- Digital Archives
- Help Desk
- Others...

***Information Security Management System
Best Practice***

e-City Evolution: Today: Multiple Points of Access



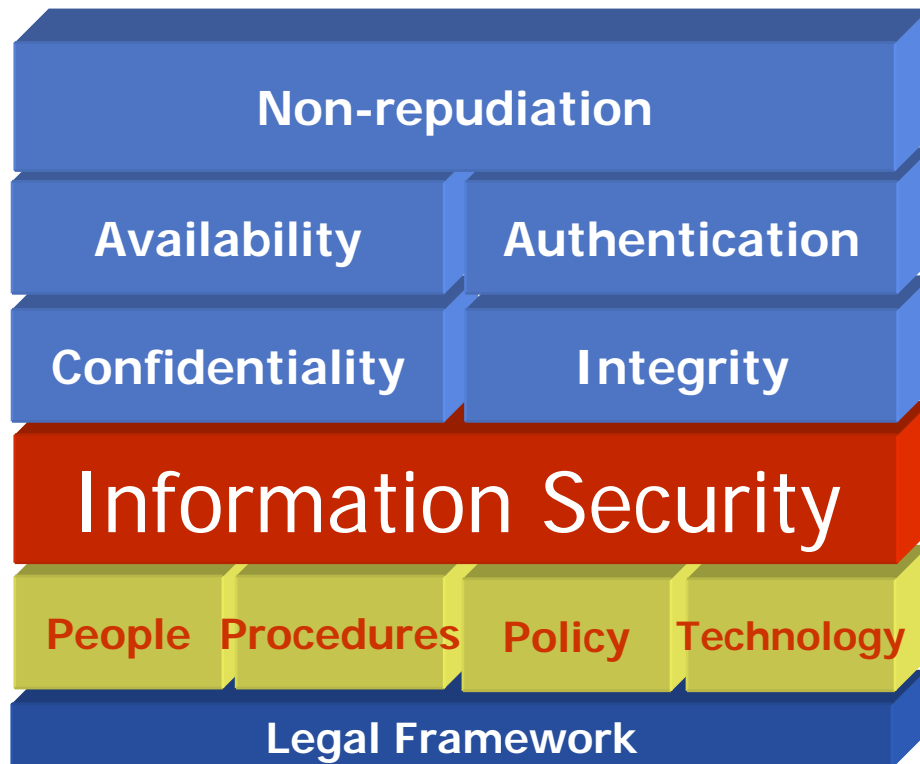
Information/Data management requirements



- **Collection**
Gathering data on citizens, businesses and other entities.
- **Storage**
Gathered data is stored for processing.
- **Processing**
Processing takes place at server level.
- **Communication**
Data collection and processing require a lot of G2C and G2B communication to happen.

Each stage above carries security risks which need to be managed!!

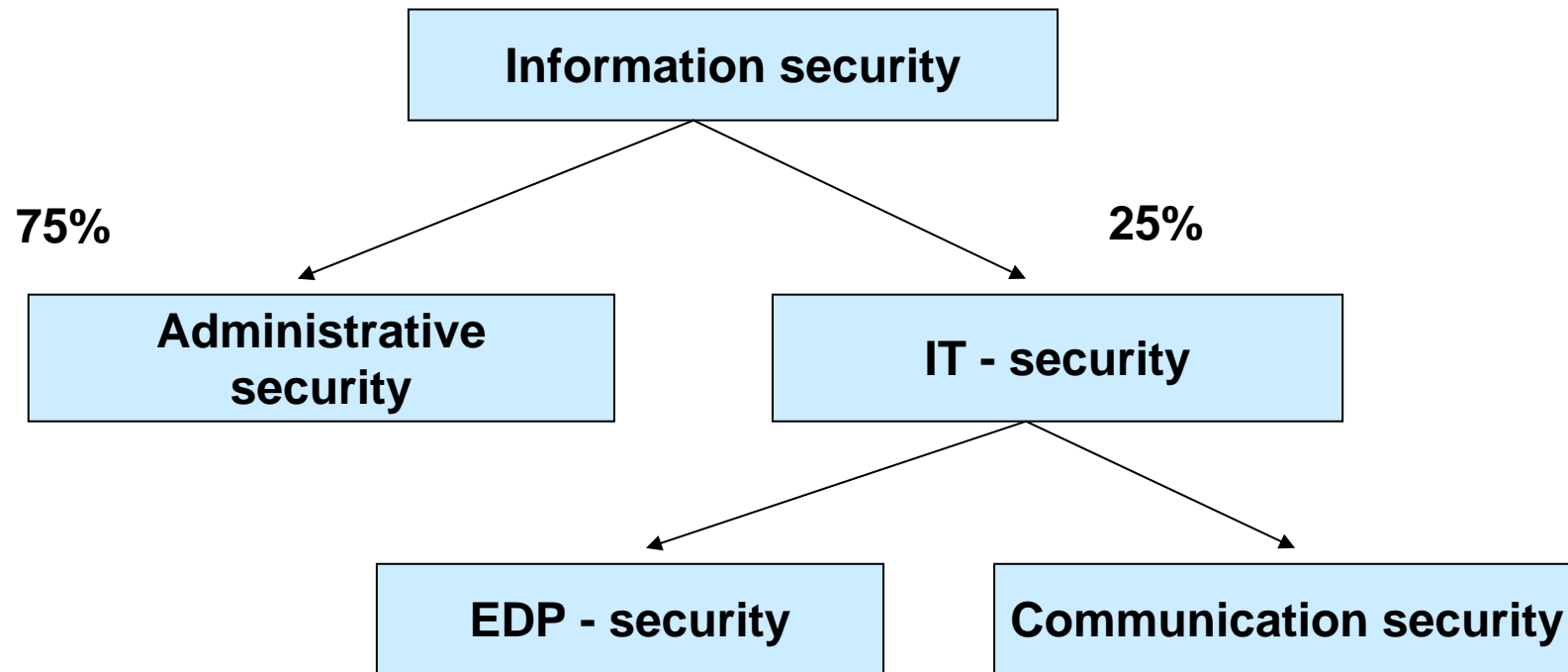
What is information security?



Information security is about preserving of confidentiality, integrity and availability of information.

BS 7799/ISO 17799

Information Security - Structure



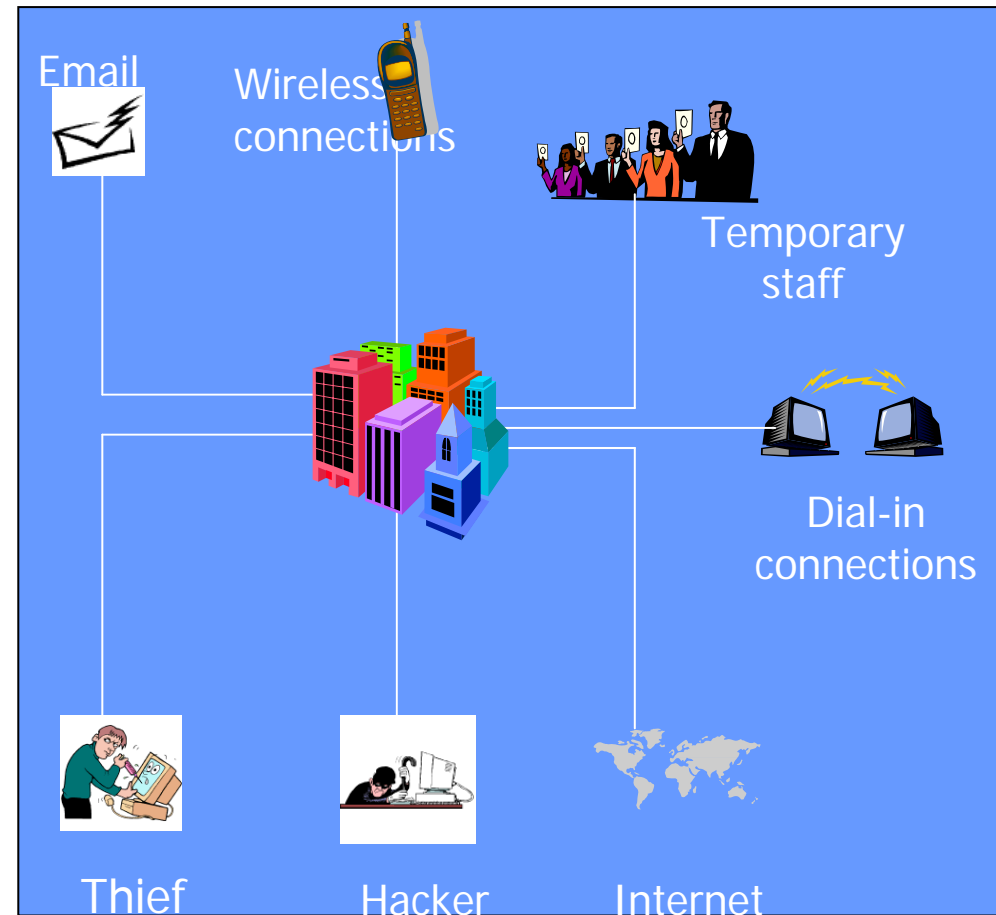
Why is information security an issue for e-City?



- Dependency on information systems
- High degree of information sharing
- Increase use of remote access
- Challenges of controlling information
- Laws relating to information security
- Dealing with highly sensitive citizen's and business data
- National security
- Consequences of security breach can be detrimental

Threats to information security in e-City environment

- Active attacks
- Passive attacks
- Viruses, trojan horses, worms
- Social Engineering
- Wireless Networking
- People
- Power
- Fire, flood, etc...

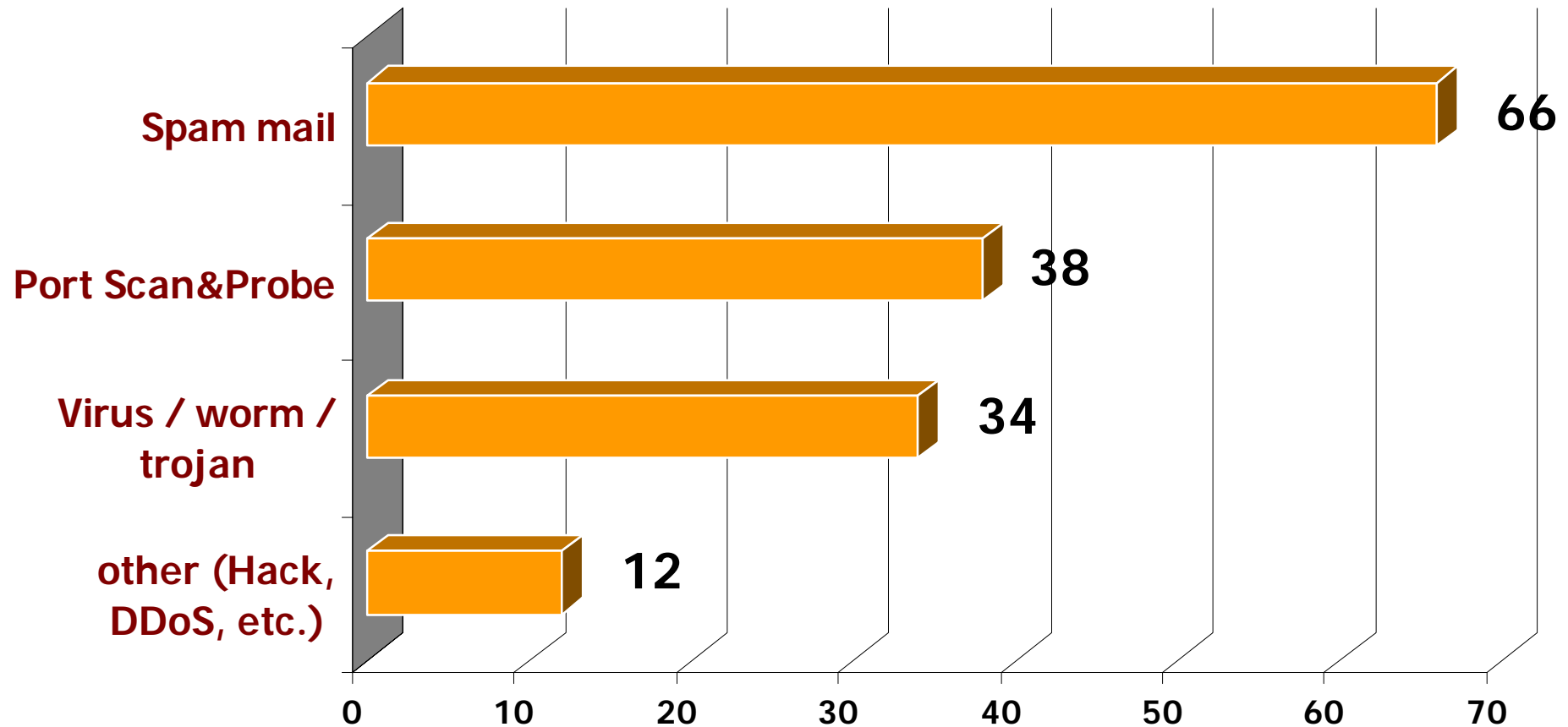


Number of Cases in year 2001

Dublin Municipality



Types of Incidents



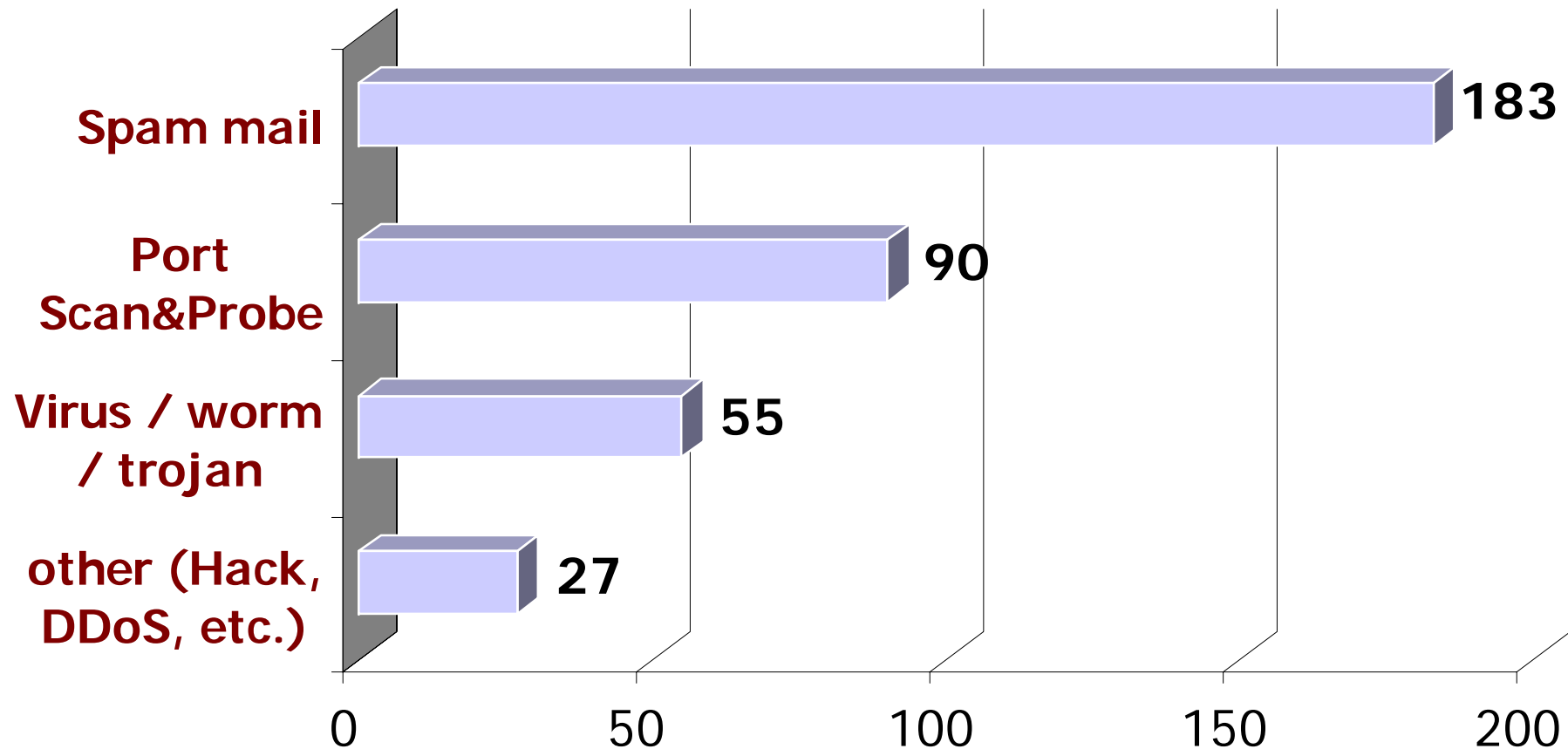
[Total = 150 cases]

Number of Cases in year 2002

Dublin Municipality



Types of Incidents



[Total = 355 cases]

Main Information Security Issues

- Only 40% of organizations are confident they would detect a systems attack. (A.9)
- 40% of organizations do not investigate information security incidents. (A.6)
- Critical business systems are increasingly interrupted - over 75% of organizations experienced unexpected unavailability. (A.8)
- Business continuity plans exist in only 53% of organizations. (A.11)
- Only 41% of organizations are concerned about internal attacks on systems, despite overwhelming evidence of the high number of attacks from within organizations. (A.6 , A.7)
- Less than 50% of organizations have information security training and awareness programs. (A.6.2)

ISO 17799:2000 defines this as the preservation of:



■ Confidentiality

- Ensuring that information is accessible only to those authorized to have access

■ Integrity

- Safeguarding the accuracy and completeness of information and processing methods

■ Availability

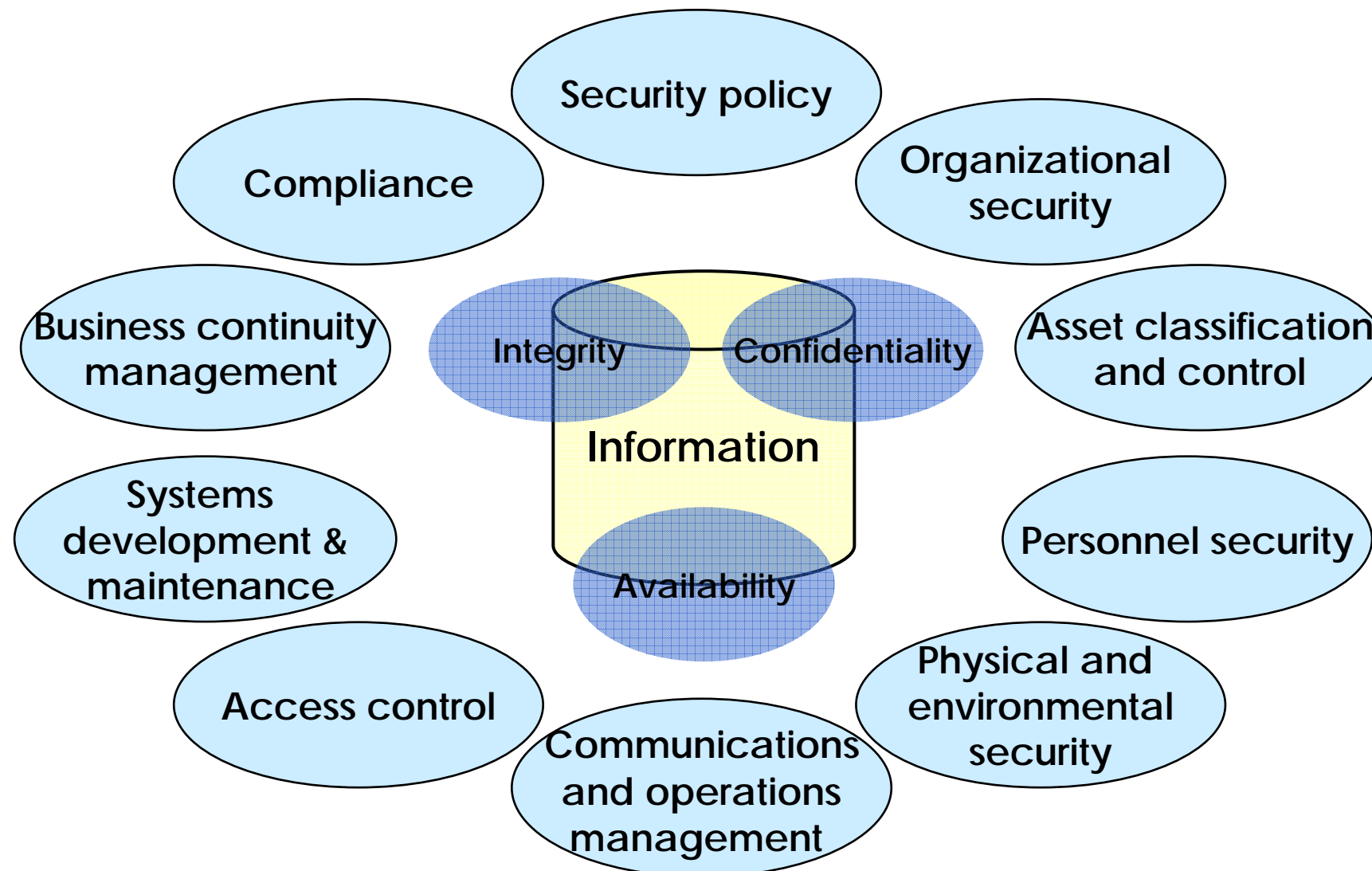
- Ensuring that authorized users have access to information and associated assets when required

Control Objectives and Controls

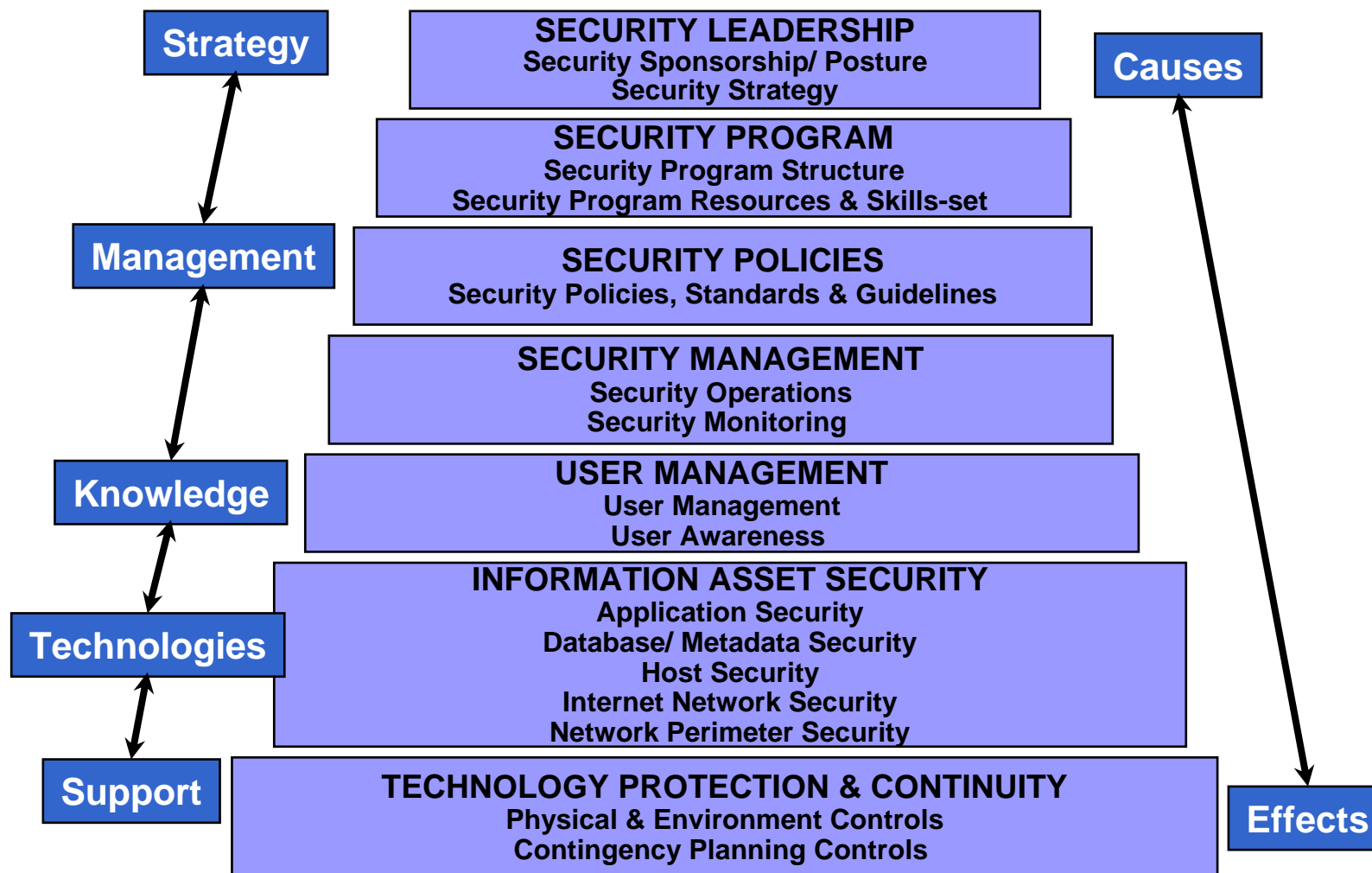
- **BS 7799-2 ISO 17799** contains:
 - 10 control clauses, 36 control objectives, and 127 controls
- “Not all of the guidance and controls in this code of practice may be applicable. Furthermore, additional controls not included in this document may be required.”
- “They are either based on essential legislative requirements or considered to be common best practice for information security.”
- “...guiding principles providing a good starting point for implementing information security.”

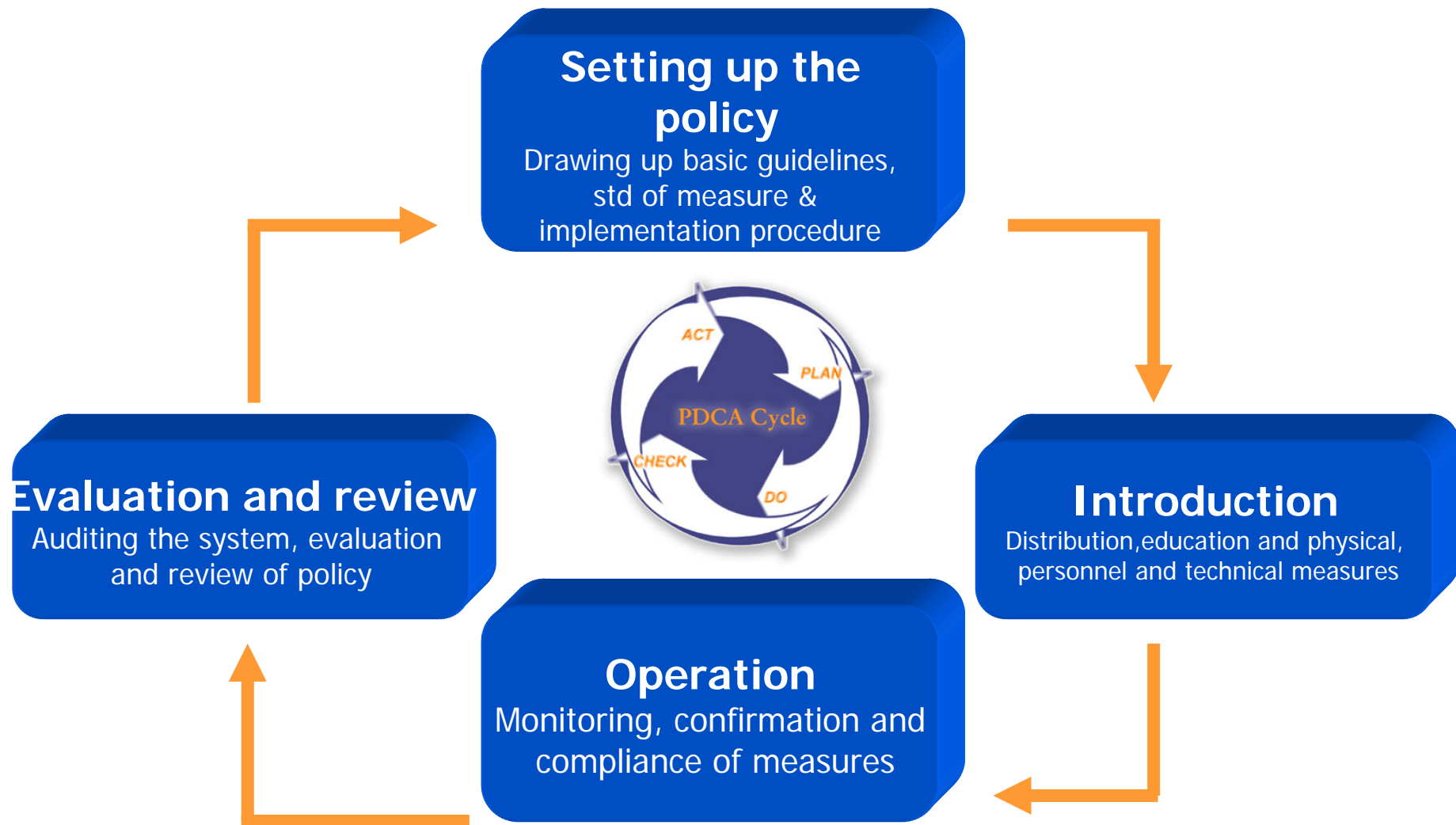


BS 7799 –10 Domains of Information Management



BS 7799 –10 Domains of Information Management (Cont.)





How to identify the security requirements?

1. From security risks
2. From legal and contractual requirements
3. From internal principles, objectives and requirements



CORRECT controls and required degree of flexibility from the START!

Implementing Information Security for e-City



- People
- Policy
- Procedures
- Technology (Public Key Cryptography – PKI)
- Risk Management
- Legal framework
- Conformity with international standards

10 key steps to securing e-City Based on BS7799



1. Assign accountability for security
2. Implement a thorough security policy
3. Conduct a security awareness program
4. Install a firewall and monitor the traffic regularly
5. Deploy anti-virus software and update it regularly

10 key steps to securing e-City Based on BS7799 (Cont.)



6. Stay abreast of security advisories and make updates in a timely manner
7. Establish strong password rules
8. Limit access to sensitive information
9. Develop and communicate an incident response process
10. Perform security audits on an ongoing basis

Improving users confidence

- PKI deployment in e-City
- Privacy / Security / Intellectual policy on City web sites
- Trust Mark Program
- Click-wrap agreement