Business Beam

What is ISO 27001 ISMS?

Business Beam

Contents

- Your Information is your Asset!
- The need for Information Security?
- About ISO 27001 ISMS
- Benefits of ISO 27001 ISMS

Your information is your asset!

What is ISO 27001 ISMS?

Information is an Asset

Information is the lifeblood for our personal activities as well as for business organizations

What is Information?

- Information is data that has been processed into a suitable form for a final user
- Information is the outcome of the processed data

Information & Business

For a business, Information is a **valuable resource**, just as much as capital infrastructure and people

Information is collected on any amount of different items and used by managers to make **strategic decisions** concerning the organisation

All information related to organizations' internal & external environment is an **Asset**

Why Information is an Asset?

Because information is recognized as **valuable** to the organization and has a certain **value**

Information is also a commodity and as such, has a monetary value, the level of which depends on its accuracy & potential use

Information helps in present & future decision making based on past trends, market research & analysis, keeping an eye on competitors and comply to regulators' requirements etc

Types of information available within an organization

- Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. It may include:
  - Market trends
  - Buying preferences
  - Customer profiles
  - Financial & Accounting records
  - Current & future business plans
  - Policies, published material etc
  - Trade Secrets
  - Partners
  - Regulators
  - Employees

What’s next?

Like other important business assets,

information is essential to an organization’s

business and consequently needs to be

suitably protected!

The need for Information Security

What is ISO 27001 ISMS?

What is Information Security?

- “Information security protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize ROI and business opportunities”.

Need of Information Security

With an increase in the use of external service providers and the adoption of new technologies, companies are increasingly getting exposed to security breach threats

In fact, 60% of respondents perceived an increase in the level of risk they face due to the use of social networking, cloud computing and personal devices in their enterprises

According to a survey, companies are taking a proactive stance as 46% companies indicated that their annual investment in information security is increasing

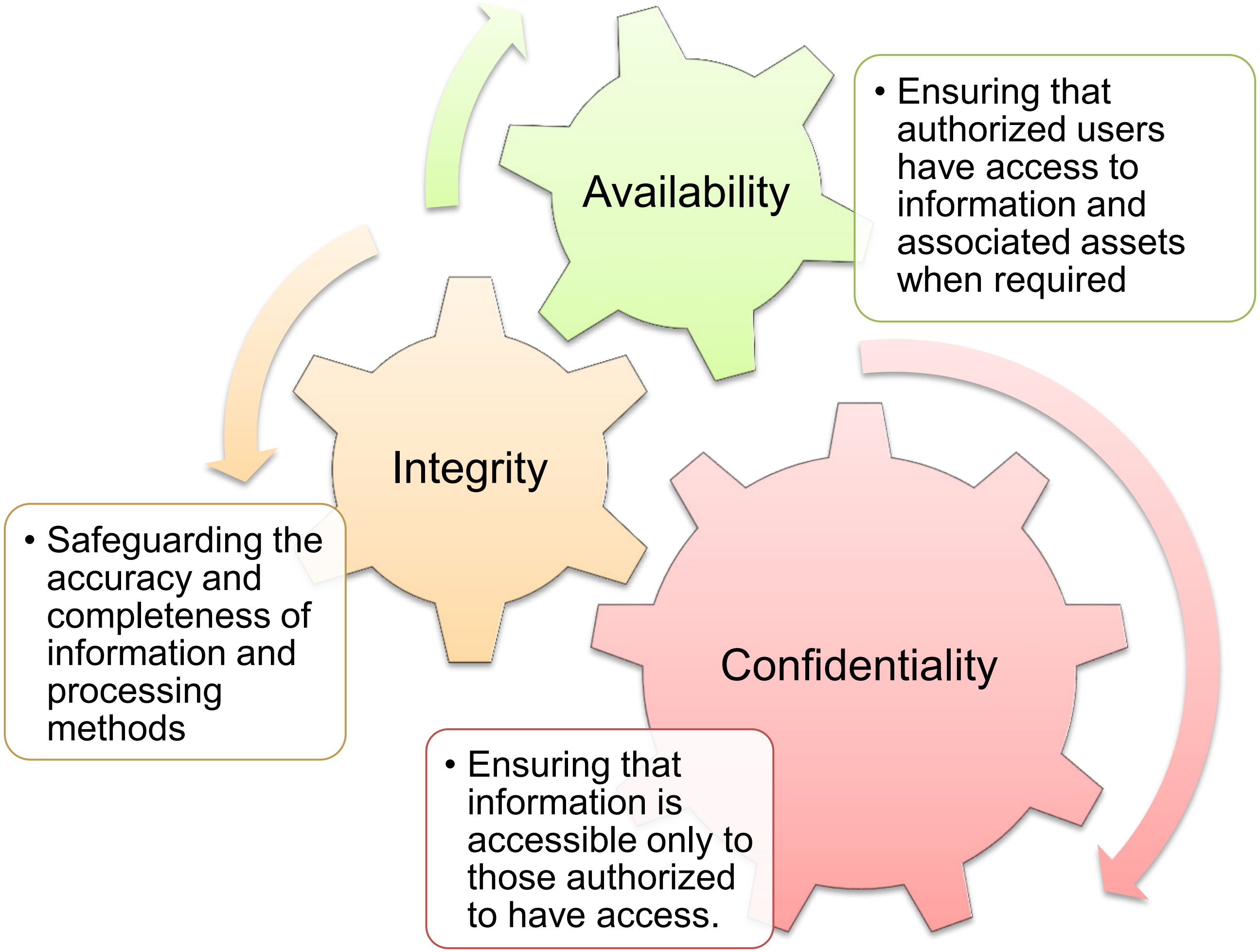
Though IT professionals are trying, but not all are succeeding in keeping up with new challenges & threats

What is information Security?

Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction

Protection of information from accidental or intentional misuse by persons inside or outside the organization

Components of Information Security



Availability

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

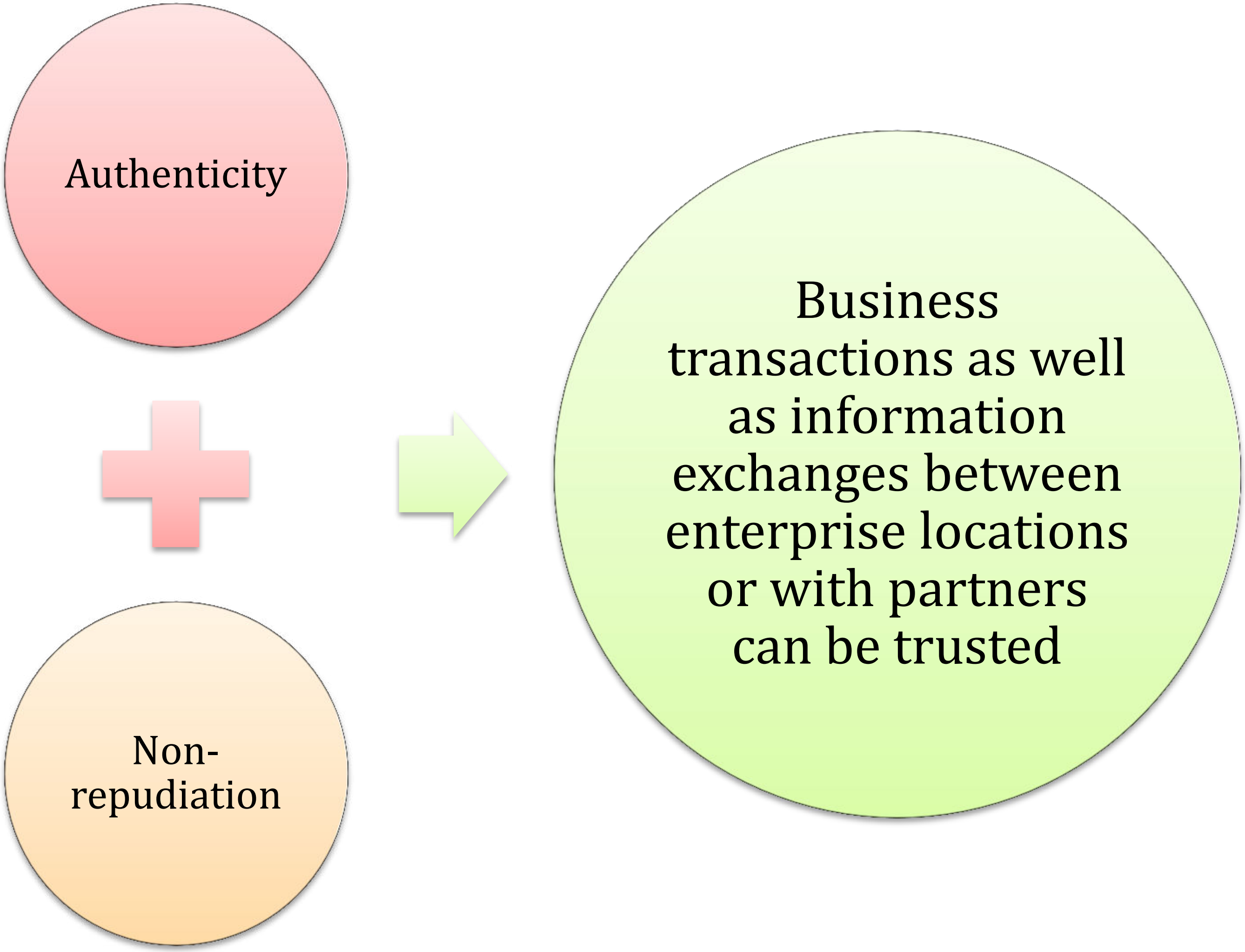
Integrity

- Safeguarding the accuracy and completeness of information and processing methods

Confidentiality

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

Information Security in Networked Economy



Authenticity

Non-repudiation

Business transactions as well as information exchanges between enterprise locations or with partners can be trusted

Consequences of Information Security Breaches

The range of undesirable consequences associated with breaches of information security is long and includes:

- Systems being unavailable
- Bad publicity and embarrassment
- Fraud
- Data damage and loss
- Corporate espionage etc .

About ISO 27001 ISMS

What is ISO 27001 ISMS?

What is ISMS?

- **“Information Security Management System is that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.”**

  NOTE: The management system includes organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

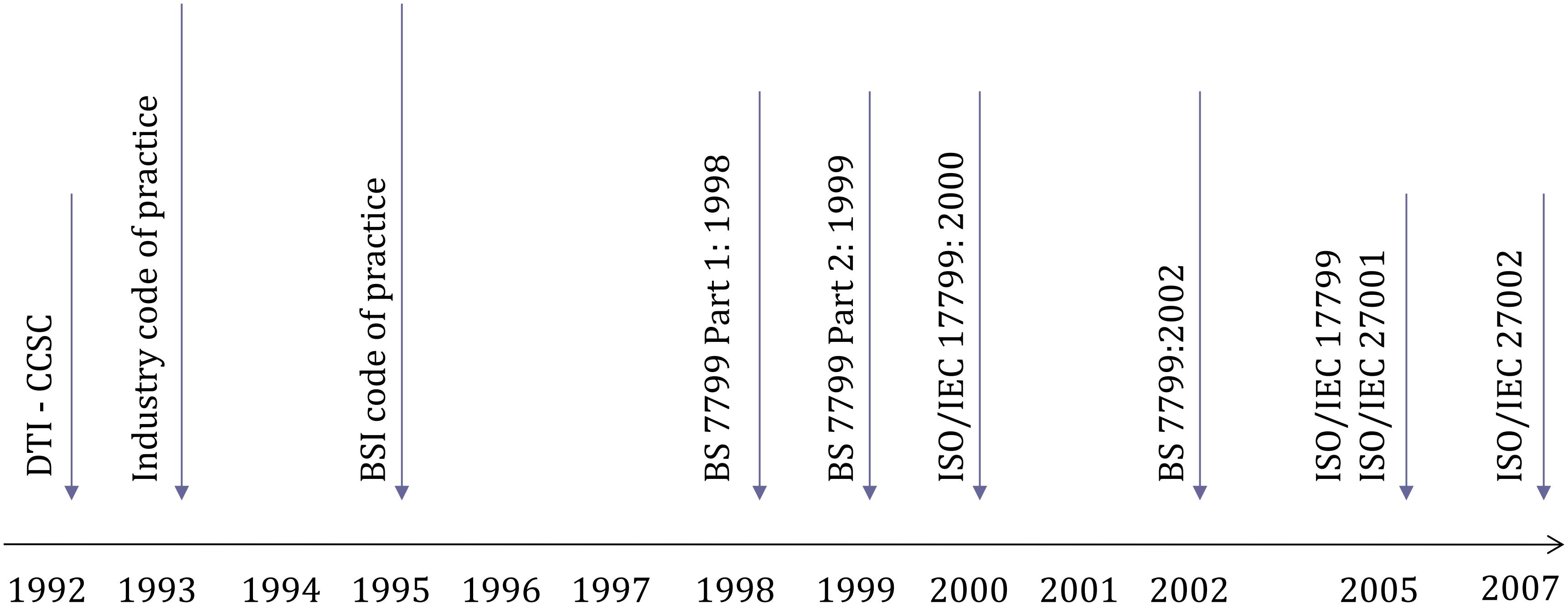
What is ISO 27001 ISMS?

- ISO 27001:2005 – Information Security Management System (ISMS) requirements

- ISO 27002:2007 – Code of Practice for Information Security Management

- The Standard:
  - Provides strategic and tactical direction
  - Recognizes that Information Security is a Management issue
  - Non-technical
  - Structured similar to ISO 9001 and ISO 14001
  - Easy Integration

History of ISO27001



DTI - CCSC

Industry code of practice

BSI code of practice

BS 7799 Part 1: 1998

BS 7799 Part 2: 1999

ISO/IEC 17799: 2000

BS 7799:2002

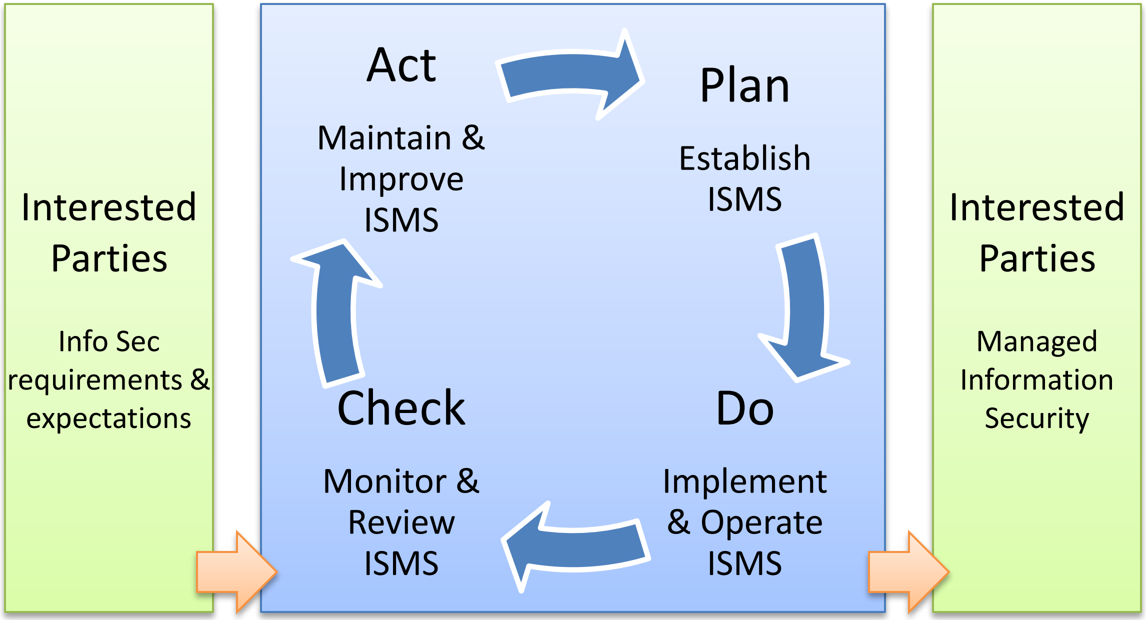
ISO/IEC 17799
ISO/IEC 27001

ISO/IEC 27002

1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2005 2007

Structure of ISO 27001

- 11 Information Security Control Areas
- 39 Information Security Control Objectives
- 134 Information Security Controls



11 Control Areas:

1. Security Policy
2. Organization of Information Security
3. Asset Management
4. Human Resource Security
5. Physical & Environmental Security
6. Communication and Operation Management
7. Access Control
8. Information systems acquisition, development and maintenance
9. Information Security Incident Management
10. Business Continuity Management
11. Compliance

ISO 27001 – Important Sections

- Section 4: Requirements
  - Establishing and managing the ISMS
  - Quality controls
- Section 5: Management Responsibility
  - Management Commitment
  - Resource Management
- Section 6: Internal ISMS Audit
- Section 7: Management review of the ISMS
  - Review input
  - Review output
- Section 8: ISMS Improvement
  - Continual improvement
  - Corrective actions
  - Preventive actions

ISO 27001 – Annex A

- Organization of Annex A
  - 11 control areas
  - 39 control objectives
  - 134 controls
- Management controls
- Technical controls
- Annex A is auditable!

ISO 27001 – Annex A (details)

- A.5 – Security Policy
- A.6 – Organization of Information Security
- A.7 – Asset Management
- A.8 – Human Resource Security
- A.9 – Physical & Environmental Security
- A.10 – Communication and Operation Management
- A.11 – Access Control
- A.12 – Information systems acquisition, development and maintenance
- A.13 – Information Security Incident Management
- A.14 – Business Continuity Management
- A.15 – Compliance

Benefits of ISO 27001 ISMS

What is ISO 27001 ISMS?

Direct Benefits

- □ Increased reliability and security of systems
- □ Increased profits
- □ Cost effective & consistent information security
- □ Systems rationalization
- □ Compliance with legislation

Direct benefits

Increased Reliability & Security of Systems

- □ Most of the business organizations nowadays are reliant on sophisticated information systems
- □ ISO27K outlines controls targeting business systems availability
- □ The controls reduce vulnerabilities from being exploited
- □ Post certification audits ensures that the business keeps up to date with latest vulnerabilities & best practices
- □ It emphasizes on continual improvement of the system which helps in making the system ‘reliable & updated’

Direct benefits

Increased Profits

- □ ISO 27001 increases business profitability from medium to long term
- □ Clients' perceptions about a certified company improves
- □ Clients' feel more secure & satisfied
- □ Clients demonstrate that a business can be trusted
- □ Some customers prefer to trade with companies who have a recognized security certification
- □ Ultimately, customers' trust & growing confidence leads to increased business profits

Direct benefits

Cost effective & consistent information security

- □ Some organizations do implement cost effective security solutions but a risk assessment under ISO 27001 actually highlights their efficiency & real effectiveness
- □ The risk assessment concludes that some of the already implemented controls offer little or no business benefits to provide an even better return off investment
- □ The risk assessment provides reconfiguration of such controls to make them more effective & even introduces some additional ones as well
- □ A non-consistency in policy framework is observed in organizations as its every division/department develops its own security guidelines
- □ ISO 27001 helps to develop a consistent approach to security
- □ It helps in creating uniform policies incorporating industry best practices
- □ A disciplinary process is also introduced to ensure employee compliance with the policies for even better results

Direct benefits

Systems Rationalization

- During the establishment phase, organizations analyze their information & information security requirements
- They simply just don’t do it
- Such analysis helps in making rational policies and spending money wisely

Direct benefits

Compliance with legislations

- Implementation of ISO 27001 forces to comply with all applicable legislations on the business
- It specially takes into consideration that the organization focuses on legalities involved in its course of business specially areas like data protection & copyright

Indirect Benefits

- Improved management control
- Better human relations
- Improved risk management & contingency planning
- Enhance customer and trading partners confidence

Indirect benefits

Improved management control

- ISO 27K emphasizes on delegation of authority
- Management effort is reduced
- Managers have more control over the organization
- They have better quality information with which they cai manage their functions

Indirect benefits

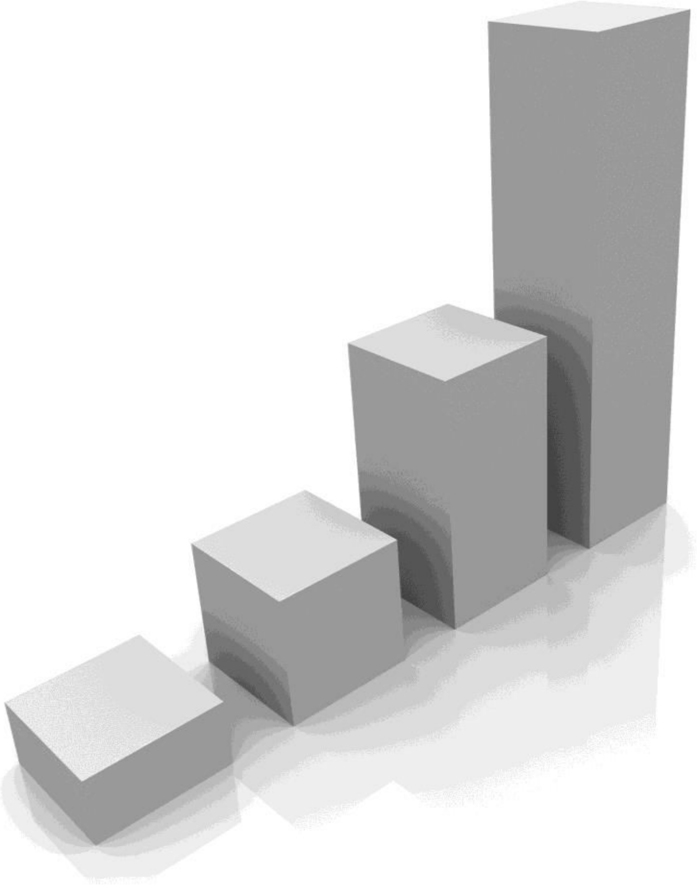
Better human relations

- □ Clear policies, procedures & guidelines make things easier and more understandable for employees
- □ Certification gives an edge to the organization over its competitors & provides it with a unique selling point that gives a better working environment to all the staff
- □ Employees start recognizing that their earning potential now depends on how customers perceive the company
- □ They get more cautious about their brand image and get extra careful while dealing with their customers
- □ Better quality human resource is employed due to established screening procedures

Indirect benefits

Improved risk management & contingency planning

- □ Through ISO 27K certification, an organization identifies its vulnerabilities, threats & potential impact
- □ Organization gets a structured approach to risk management
- □ The risk assessment identifies which risks are more critical for the success of the business
- □ It helps in making a business continuity & DR plan which reduces the potential exposure to financial loss or negative publicity



Indirect benefits

Enhanced customer & confidence

- □ Helps in standing out from the competitors
- □ Certification provides an impression of a more trusted trading partner which is responsive to security breaches
- □ Having ISO27K logo on the company literature is a continual reminder to potential & existing clients that we are an organization which takes the confidentiality, integrity and availability of their & our information seriously

Business Beam

Thank you!

contact@businessbeam.com