# ISO/IEC 27001

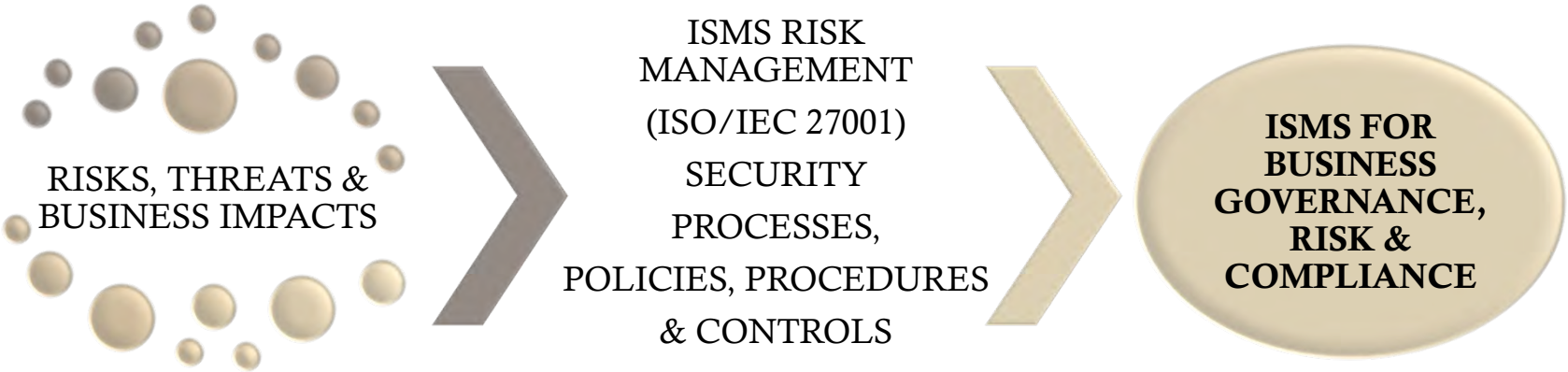
*A Global Success, A Corporate Benefit and A Competitive Advantage*

Prof. Edward Humphreys
Convenor of ISO/IEC JTC 1/SC27/WG1

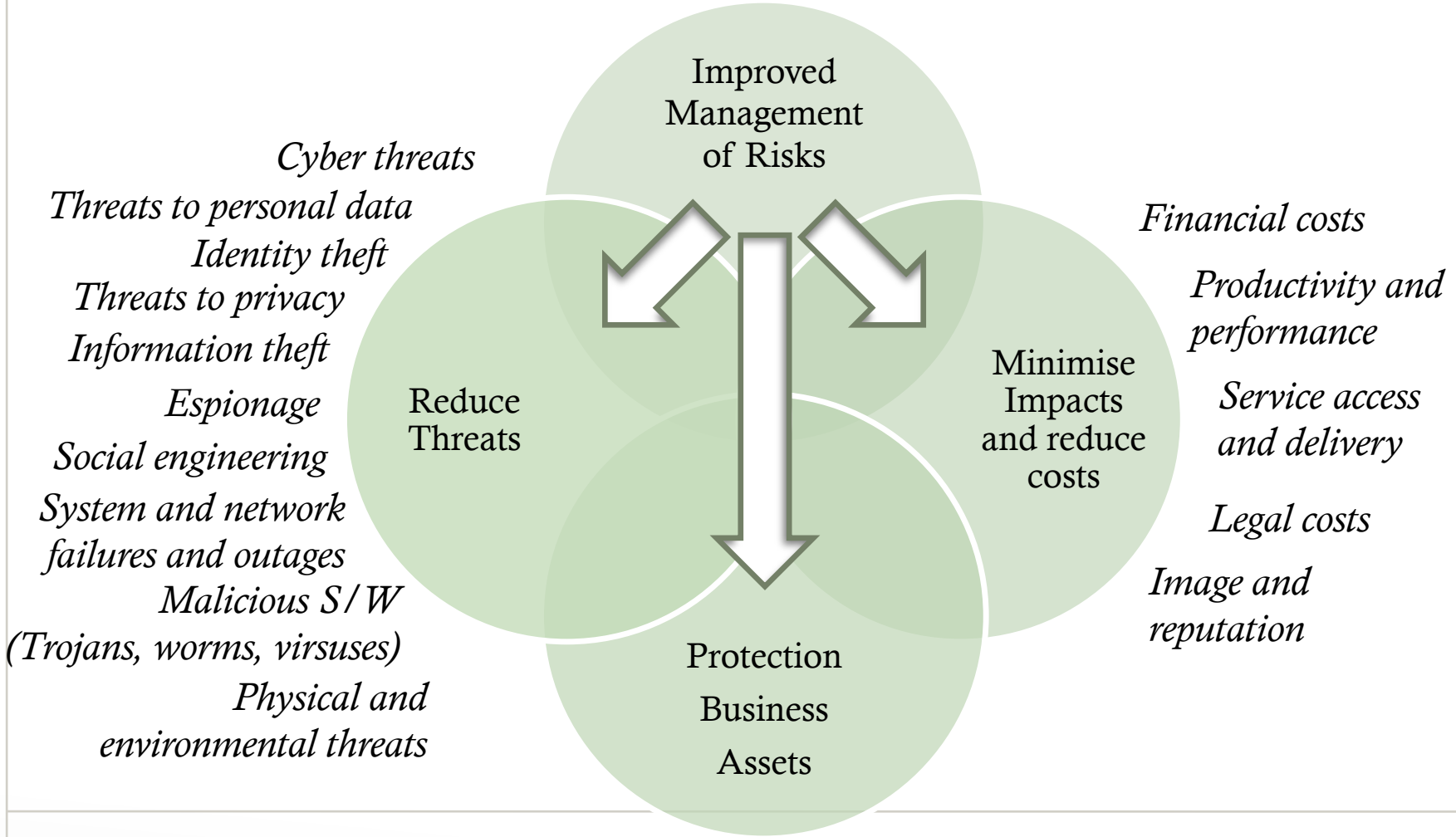
Pacific Accreditation Cooperation (PAC)
Hong Kong, 18th June 2012

# What is ISO/IEC 27001?

- Information Security Management System (ISMS) standard
- Used for accredited certifications
  - ISO 17021& ISO/IEC 27006, ISO 19011 & ISO/IEC 27007
- Based on risk-management processes, information security controls and effective continuous improvement

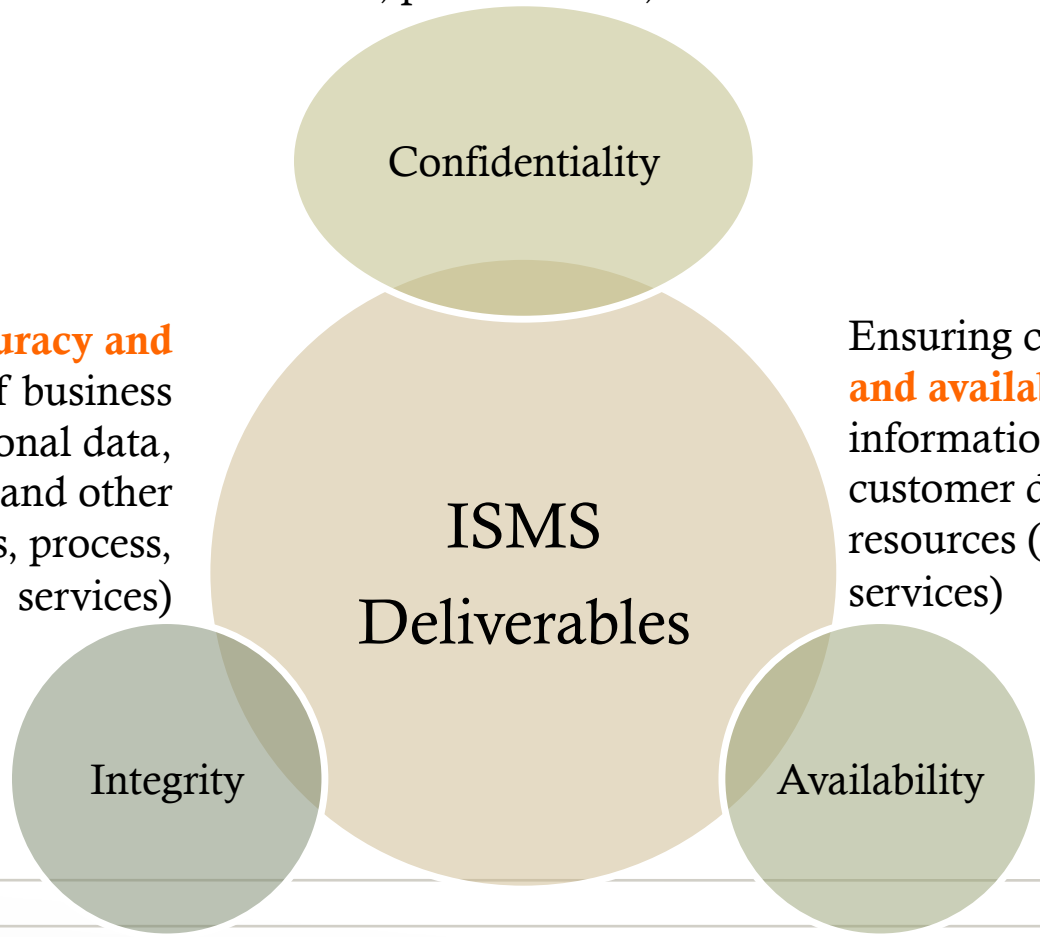


# Proven Business Security



# Proven Business Security

Ensuring **only authorised users have access** to business information, personal data, customer data …



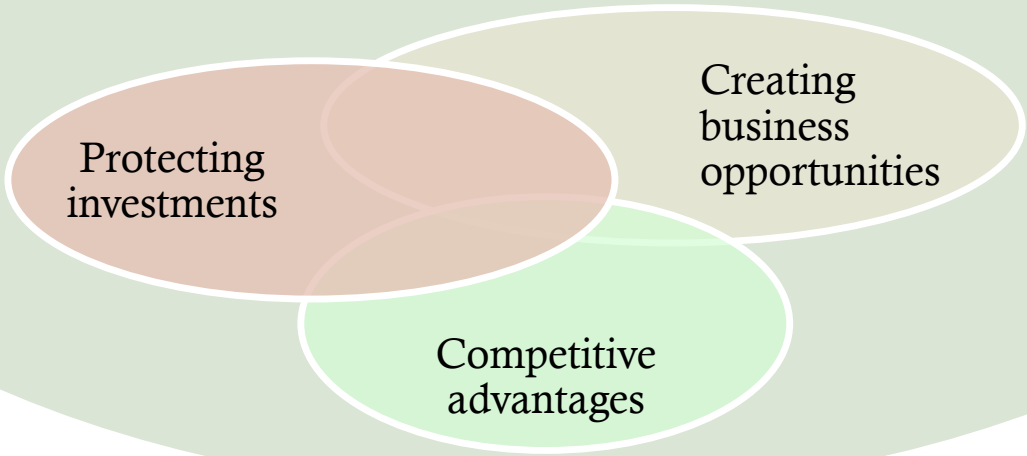

Ensuring **accuracy and correctness** of business information, personal data, customer data and other resources (systems, process, services)

Ensuring continuous **access and availability** of business information, personal data, customer data and other resources (systems, process, services)

# Proven Return on Security Investment

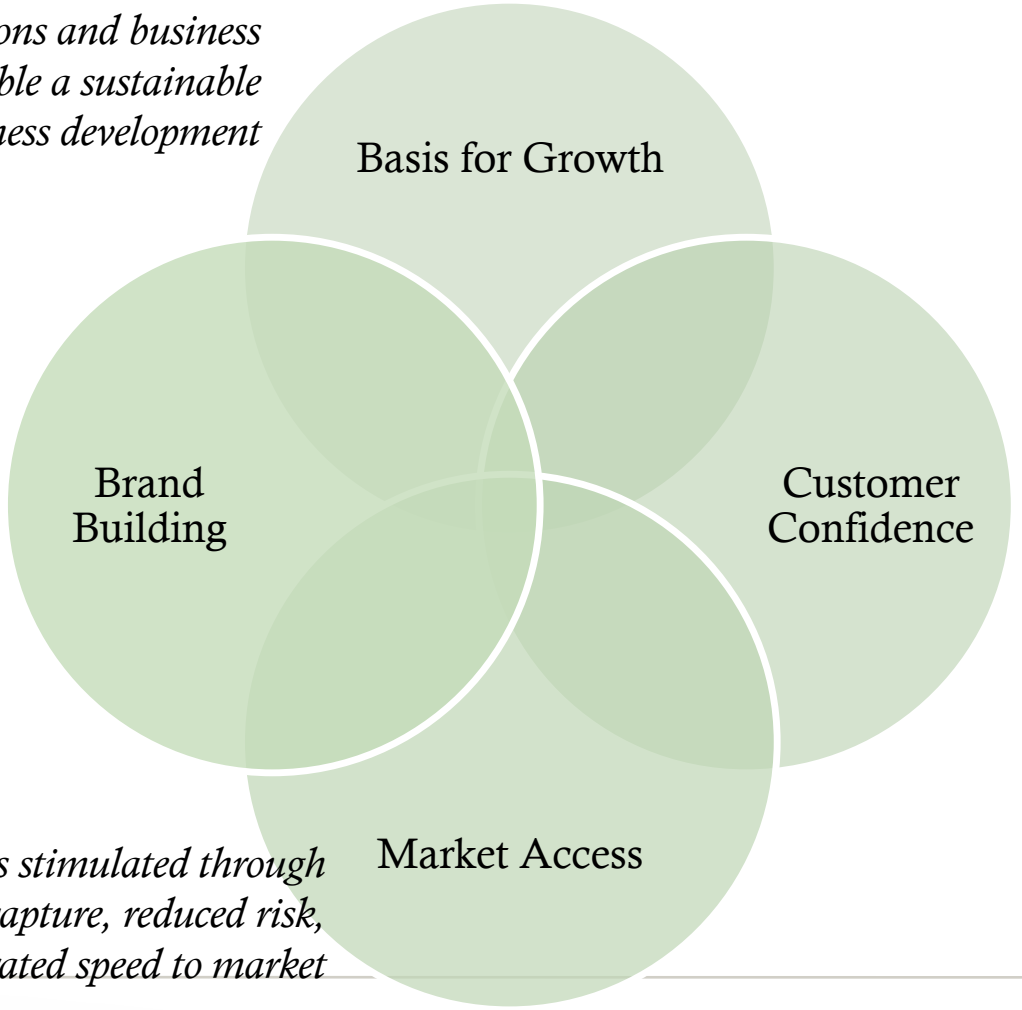
Improved protection of business assets

- More effective use of security processes and controls
- Measurable reductions in data loss or damage, security incidents, business disruptions and risks to assets
- Maximising business use, application and availability of business resources



# Proven Business Benefits

*secure operations and business continuity enable a sustainable base for business development*

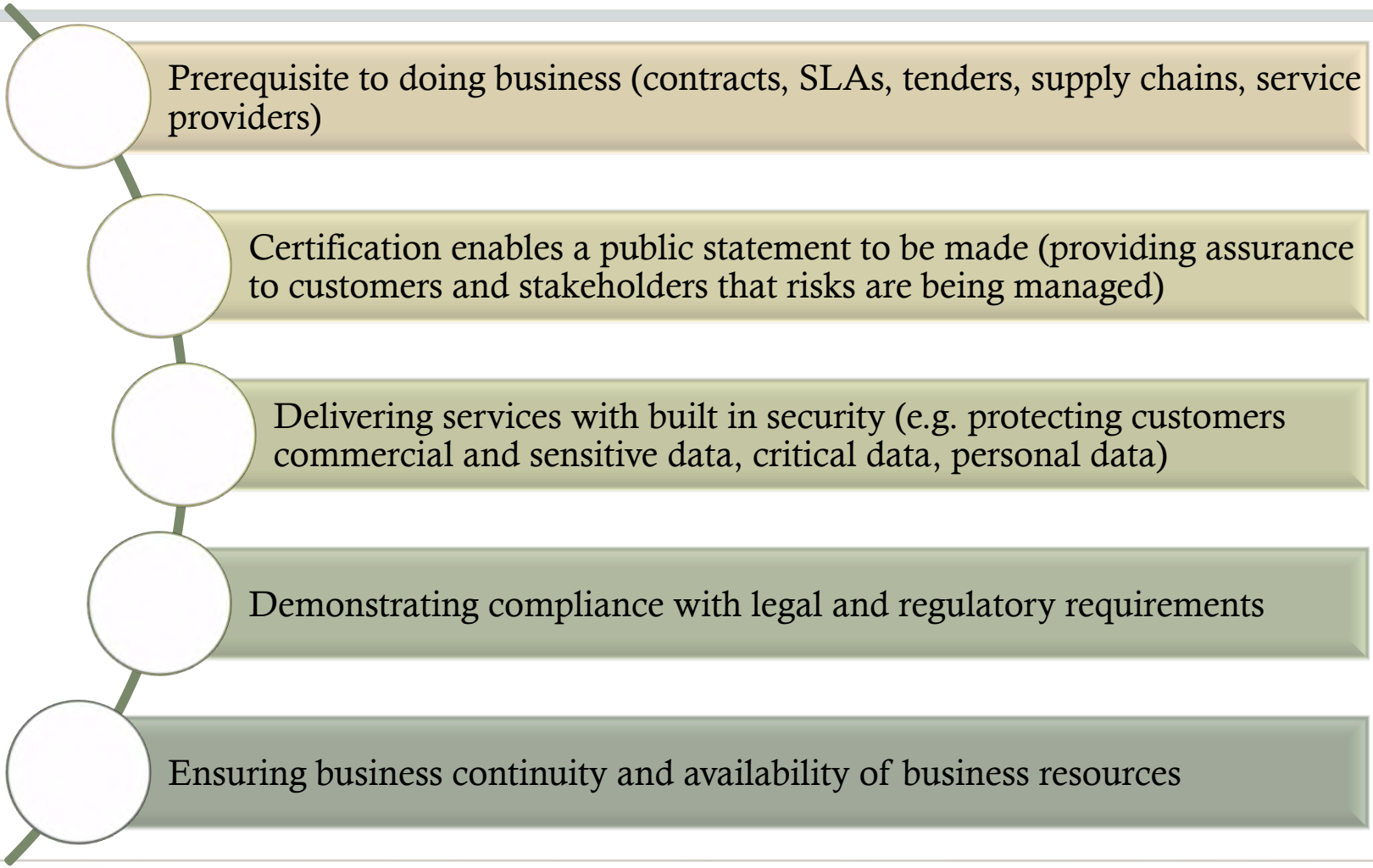



*consumer confidence in effective security strengthens the business brand(s)*

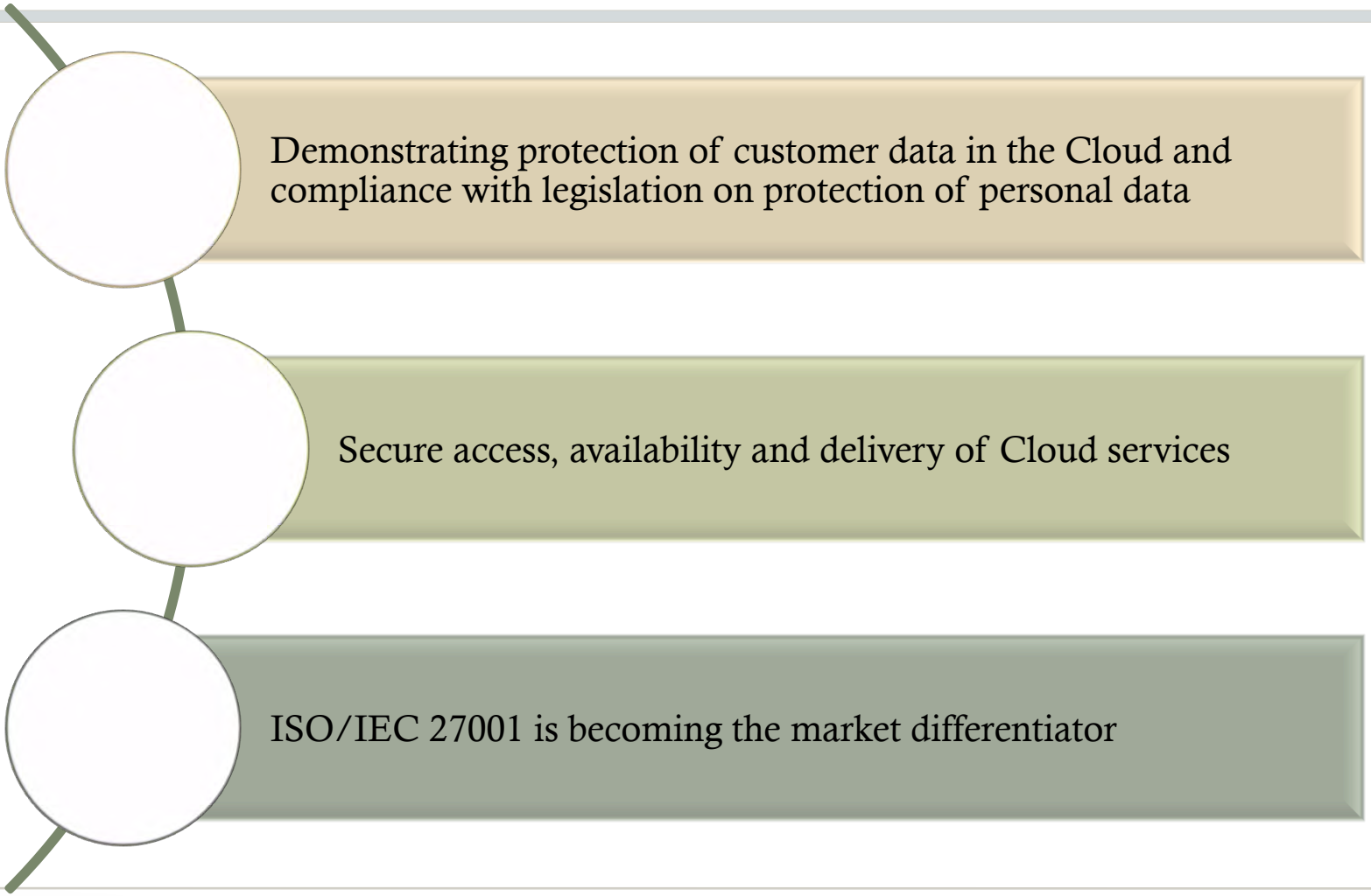
*assurance and continuous improvement of security, risk management, and effectiveness*

*competition is stimulated through knowledge capture, reduced risk, innovation and accelerated speed to market*

# Increasing Competitiveness



# Increasing Competitiveness (Example – Cloud and Web Services)



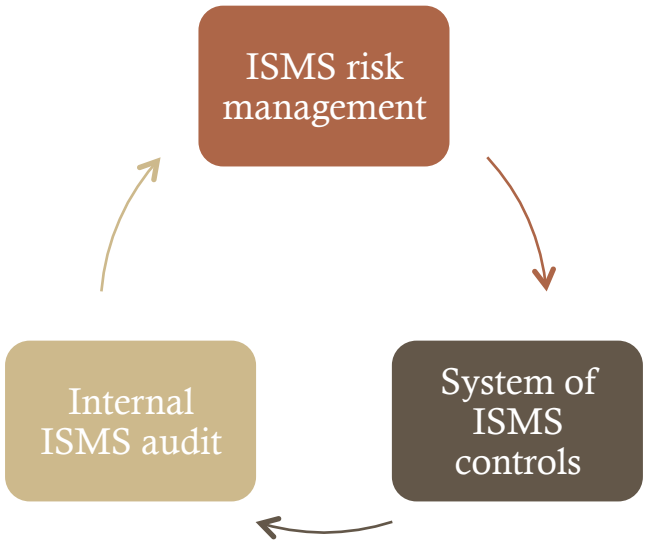
# Showing Commitment through ISO/ IEC 27001 Certification

Public statement of the commitment to ISMS governance of the organisation

Proves the commitment of your organisation's CEO, senior management, governing board to ISMS

Commitment to proper the identification, analysis and management of the organisation's ISMS risks

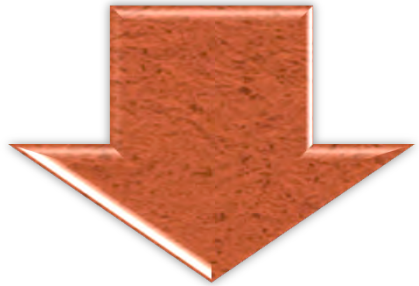
Commitment to the regular monitoring and review of the effectiveness of the organisation's ISMS



# Operational Benefits through ISO/IEC 27001 Certification

Increases operational effectiveness and performance

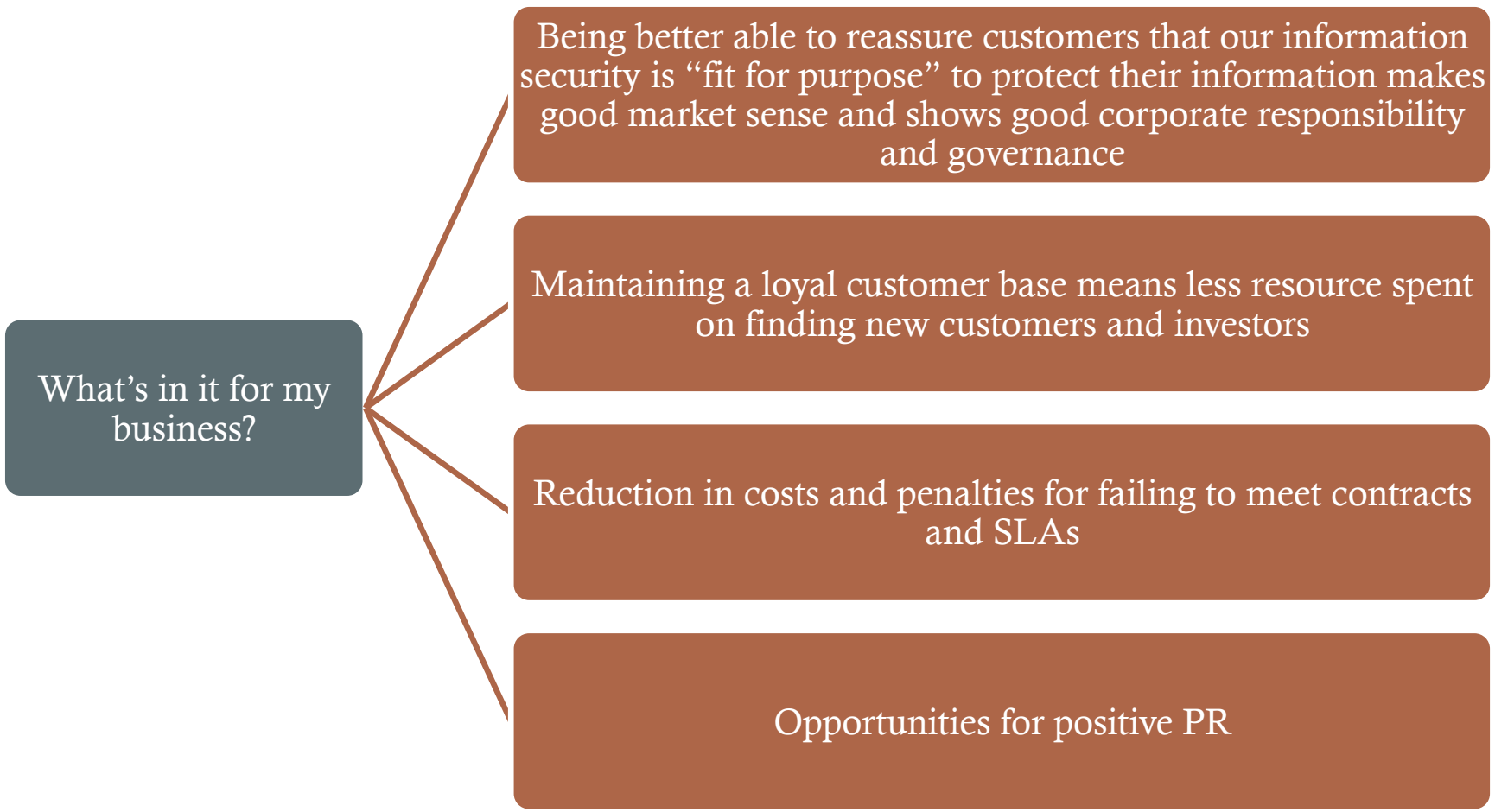
- More time spent on pro-active operational process than needing to recover from the affects of security incidents
- Less interruptions means greater productivity and performance
- Greater staff awareness of leading to staff being able to more likely to spot and avoid potential security risks and incidents.



Decreases the impact of incidents and business disruptions

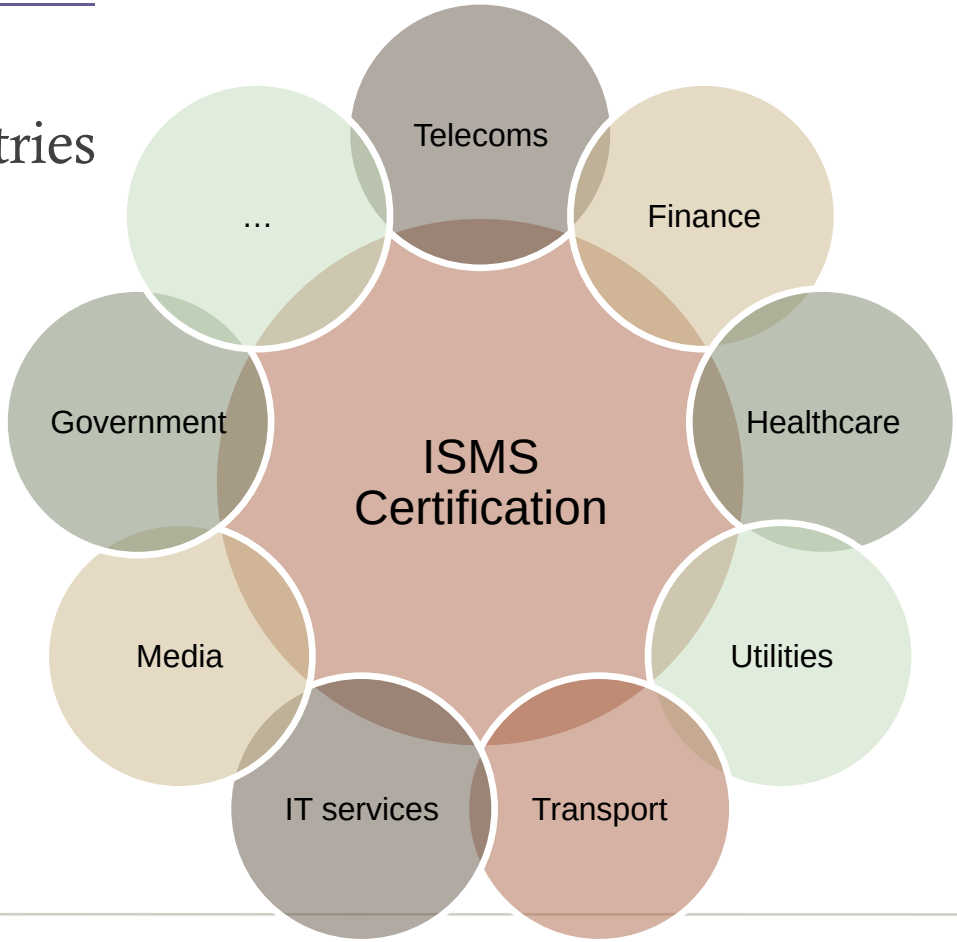
- Being ready and prepared in the event of a security incident means quicker response times and less operational impact.
- Less time spent on responding to security incidents
- Decrease in the costs and resources needed to resolve security incidents

# Customer Confidence through ISO/ IEC 27001 Certification

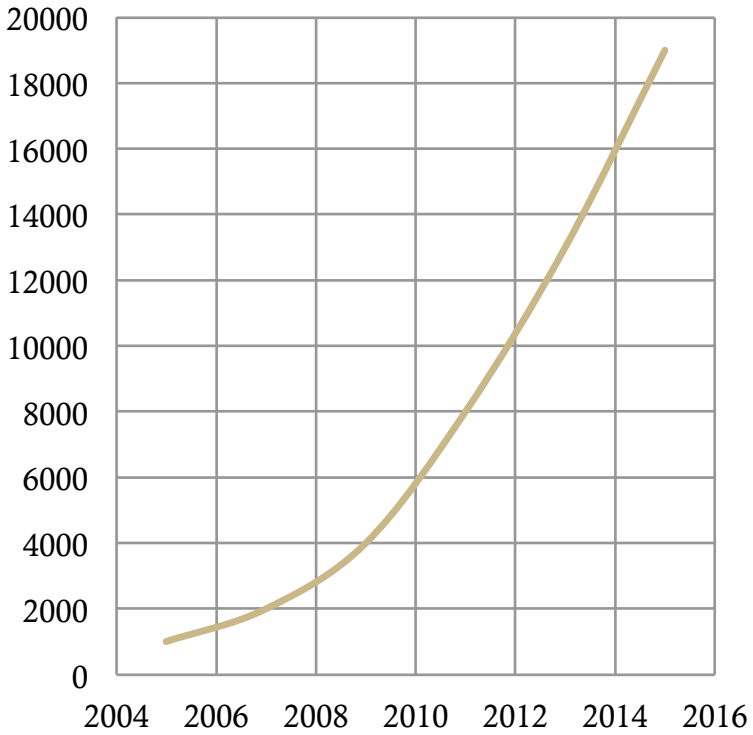


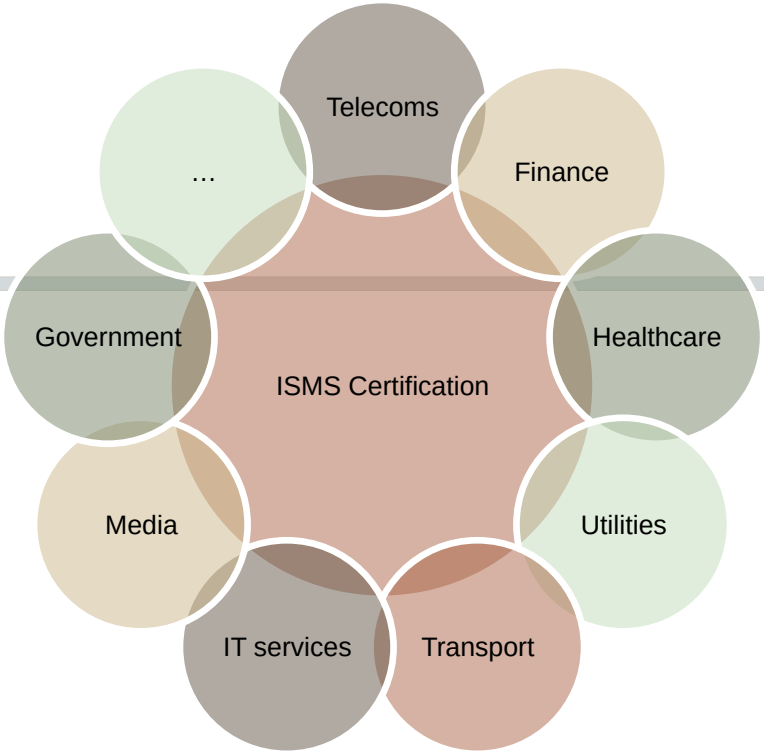
# Certifications

- www.ISO27001certificates.com
- Small, medium and large organisations from 86 countries
  - Japan
  - UK
  - India
  - China
  - Taiwan
  - Germany
  - Czech Rep.
  - Rep. of Korea
  - USA
  - Italy
  - Spain
  - …



# Certifications




- …. Telecoms (British Telecom, China Telecom, France Telecom KDDI, Korea Telecom, KPN, NTT, PCCW, T-Systems, …)
- Banks (Banque de France, China Construction Bank, Citi Bank, Federal Reserve Banks, World Bank … )
- Vendors (Amazon Web Services, Google Apps Services, HP, IBM, Microsoft Office 365, Ricoh, Samsung, SAP, Siemens, Sony, Sun, Toshiba, Unisys, Xerox ….)
- Government Depts. (Australia, Canada, … Germany, Hong Kong, Italy, … Spain, … UAE, UK, USA), UN
- Electricity, water and gas suppliers, Oil companies (Shell …. Airlines, railways, road systems … Hospitals and health service suppliers ... Bechtel, Deutsche Post, Hyundai, Reuters HK and SA ….

# Future Developments

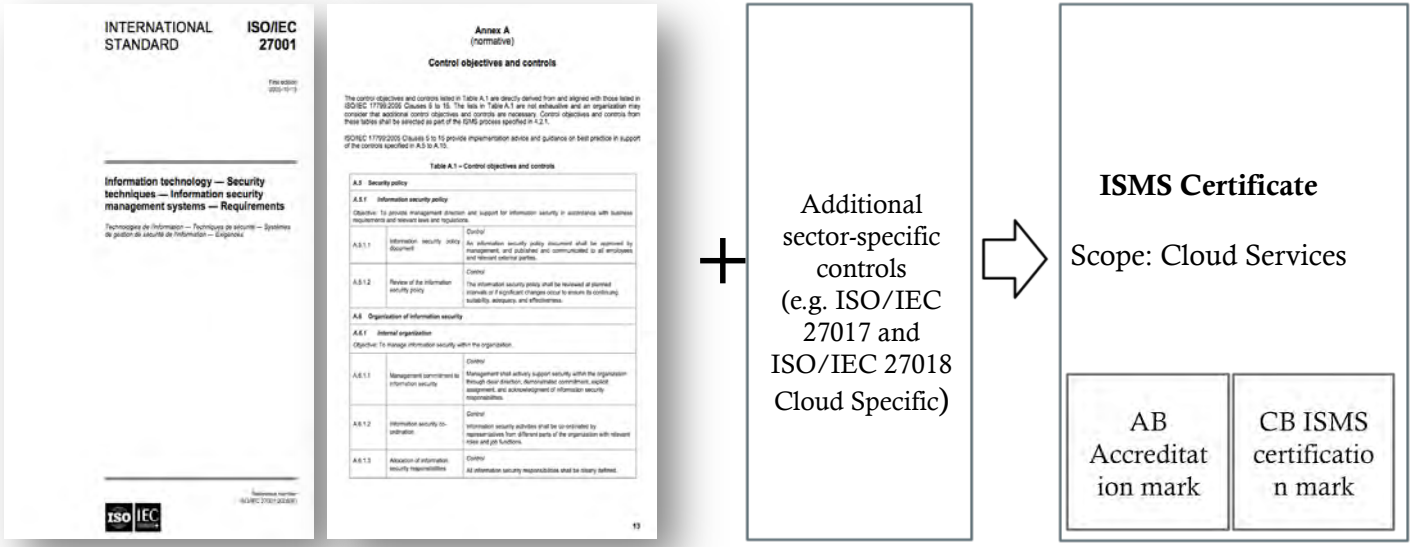
- ISO/IEC 27001: 2005 currently under revision
  - Adopting TMB Guide 83 (which is now Annex SL of the ISO Directives)
    - harmonized structure
    - common text
    - common terminology for all MSS
- ISO/IEC 27006: 2011 *(Requirements for bodies providing audit and certification of information security management systems)* is currently under revision to align with the revision of ISO 17021

# Future Developments

- Development of Sector Specific Standards for ISO/IEC 27001 Certifications
  - Cloud Computing *(ISO/IEC 27017/27018)*
  - Protection of Personal Data
  - Telecoms *(ISO/IEC 27011)*
  - IT Service Management *(ISO/IEC 27013) – ISO/IEC 20000-1 & ISO/IEC 27001*
  - Finance *(ISO/IEC 27015)*
  - Smart Grid …

# Future Developments

- Development of Sector Specific Standards for ISO/IEC 27001 Certifications
  - Cloud Computing *(ISO/IEC 27017/27018)*




ISMS processes + controls

Thank You
For Listening

❖

Any Questions