Information Security Management Systems Standards

ISO/IEC 27001

Global Opportunity for the Business Community

Prof. Edward (Ted) Humphreys

IPA Global Symposium 2013

23rd May 2013, Tokyo, Japan

IPA Information-technology Promotion Agency, Japan

- CyberSecurity and ISO
- Reminder of what ISO/IEC 27001 is
- Revision of ISO/IEC 27001
- Next Generation of Management Systems
- Integrated management systems
- Global certification
- Sector-specific certifications
- Update on the Family of ISO/IEC 27001 standards

CyberSecurity and ISO

- Cyber attacks have an impact on all our lives and well being
  - Affecting all sectors – Business, Government and all areas of society
  - Resulting in damage, harm and disabbling of national infrastructure (telecoms, finance, transport, energy, food supply, healthcare, social services …)
  - Hence there are political, social and economic consequences
- What are the risks/impacts/solutions?

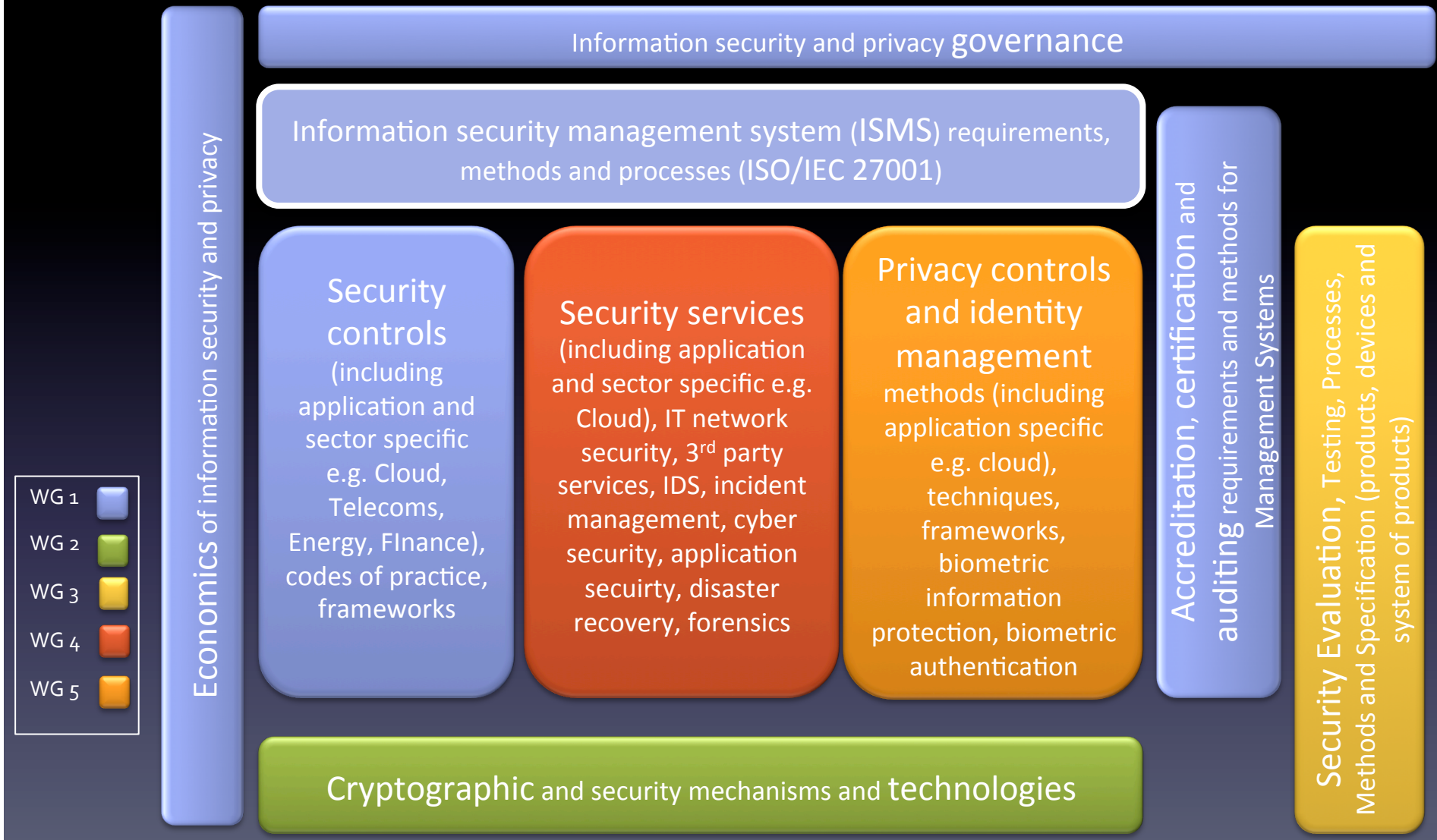
IPA

CyberSecurity and ISO

- International standards have a significant role to play in delivering solutions
  - Common international language
  - Effective interworking and integration
  - Efficient deployment and sharing of resources
- Standard solutions
  - GRC (Governance, Risk and Compliance)
  - Management, Controls, Services, Technology

IPA

ISO - BIG Picture Standards Map



ISO/IEC JTC 1/SC27 programme of work

IPA

What is ISO/IEC 27001?

- **27001** is an **Information security management system** (ISMS) standard (a GRC standard)
  - Protecting the confidentiality, integrity and availability of assets
  - Minimising information security risks
  - Maximising business opportunities and investments
  - Ensuring business continuity of systems and processes

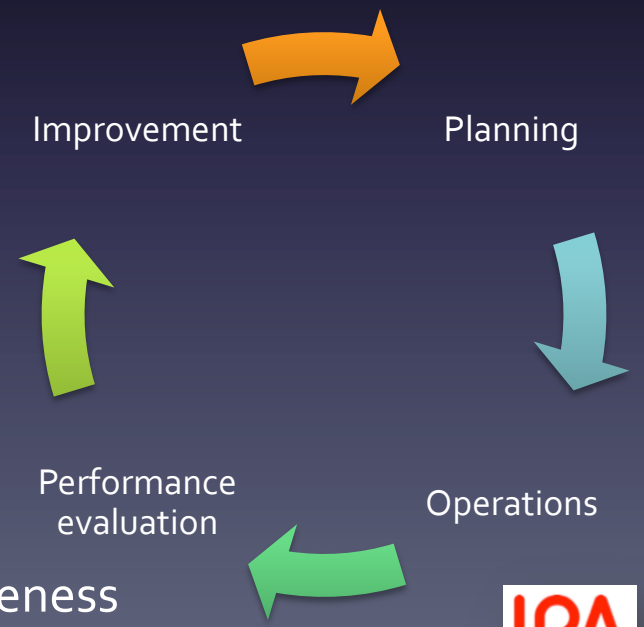
IPA

What is ISO/IEC 27001?

- It is a *risk based management tool* for managing information security risks which encompasses the business process, critical system elements and critical system boundaries
  - Controls are implemented to establish an effective level of information security to mitigate the risks

What is ISO/IEC 27001?

- It involves a *continuous improvement programme* to maintain the effectiveness of an organisation's information security management to meet changing risk and threat environments
  - Identify the risk profile
  - Implementing controls to mitigate against the risks
  - Monitoring, measuring and reviewing the effectiveness of these controls
  - Making control improvements to the effectiveness



IPA

What is ISO/IEC 27001?

- Finally - 27001 provides the framework for 3rd-party audits and certification of an organisation's ISMS
  - Demonstrating you take cyber-security, Cloud security seriously
  - Providing 'fit-for-purpose' and 'duty of care' confidence and assurance to customers and stakeholders
  - Verifying your governance and risk management programme is effective

IPA

Revision of ISO/IEC 27001 ISMS

- The first edition of 27001 was published in 2005
- What has happened since 2005?
  - Increase in cyber risks and on-line crime
  - Advances in technology
  - Greater use of mobile services and networks
  - More laws and regulations …
  - … etc
  - And the development of a specification for the Next Generation of Management System Standards

IPA

Revision of ISO/IEC 27001 ISMS

- In 2009 it was decided to start work on a revision
  - Update the standard so it remains current and useful to users
    - *Feedback from users and interested parties on practical experiences and effectiveness of ISMS implementations*
    - *Certification experiences*
  - To be aligned with the move towards the **Next Generation of Management System Standards**
- **2013 will see the release of the revised version**

IPA

So What is the Next Generation of Management System Standards (NG-MSS)?

The NG-MSS is a trend towards harmonised, integrated and consistent management systems.

- All ISO management system standards will in the future be aligned according to an agreed high level structure, identical core text and common terms and core definitions *(ISO/IEC Directives Part 1, Annex SL, Appendix 3)*.

This will increase the value of such standards and be particularly useful for organisations that operate across multiple management system platforms.

IPA

Next Generation of Management System Standards

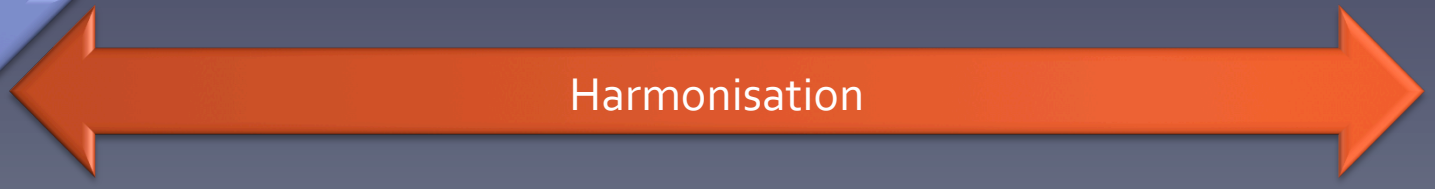
- Trend towards harmonised, integrated and consistent management systems offering
  - Greater trade opportunities
  - Economies of scale through integrated scopes, policies and procedures
  - Maximising business investments and minimising business costs through integrated management systems
  - Improved operations through integrated performance evaluations

Next Generation of Management System Standards

- Better management of risks through integrated platforms and infrastructure
  - Function: Quality, environment, information security, business continuity
  - Sector: Telecoms, Finance, IT services, Energy, Manufacturing, Transportation, Healthcare …

Next Generation of Management System Standards (Examples)

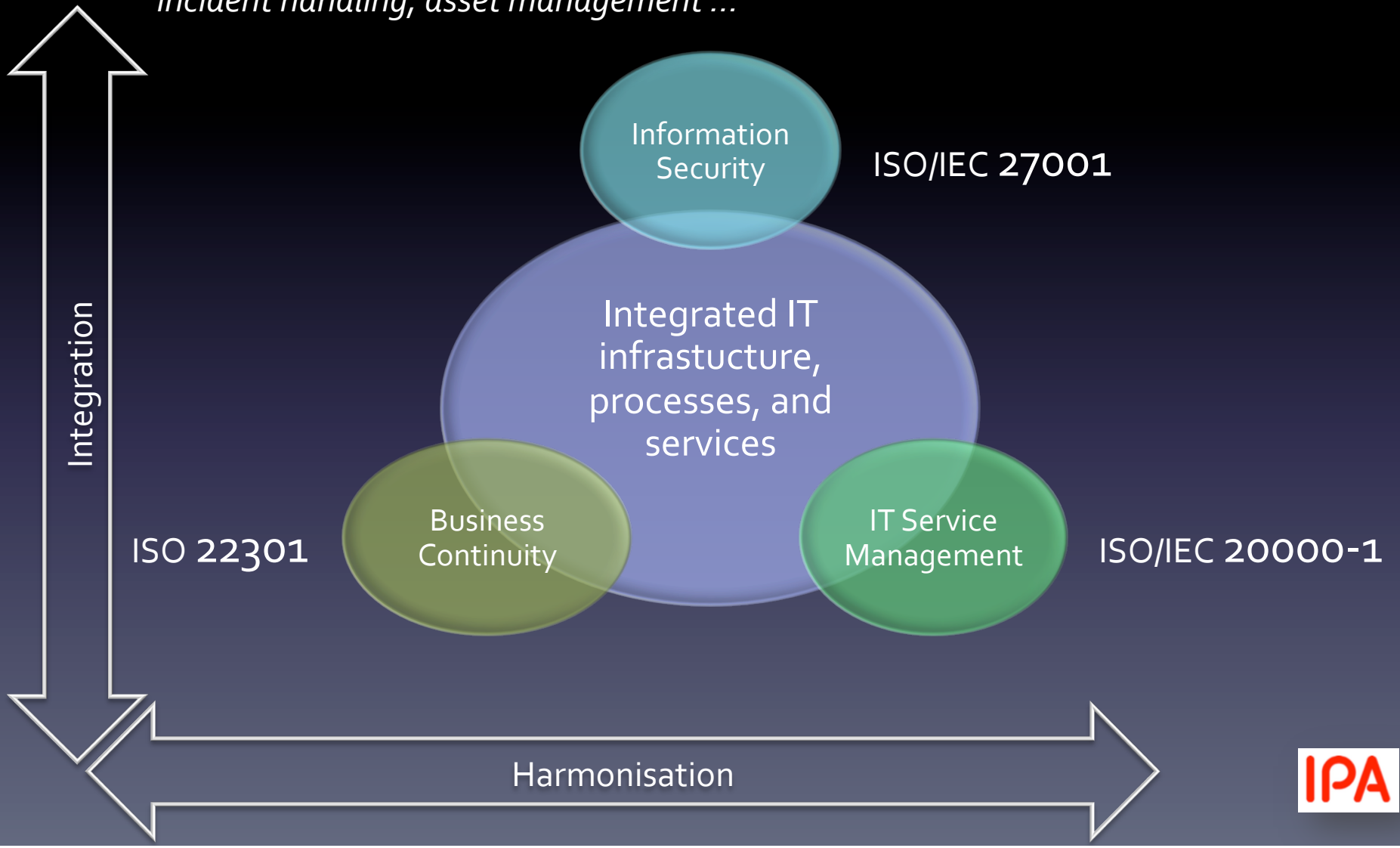
- ISO 9001 (quality)
- ISO 14001 (environment)
- ISO/IEC 20000 (IT service management)
- ISO 22301 (business continuity)
- ISO/IEC 27001 (information security management)
- ISO 29001 (oil and gas management)
- ISO 39001 (road safety management)
- ISO 50001 (energy management)
- … etc



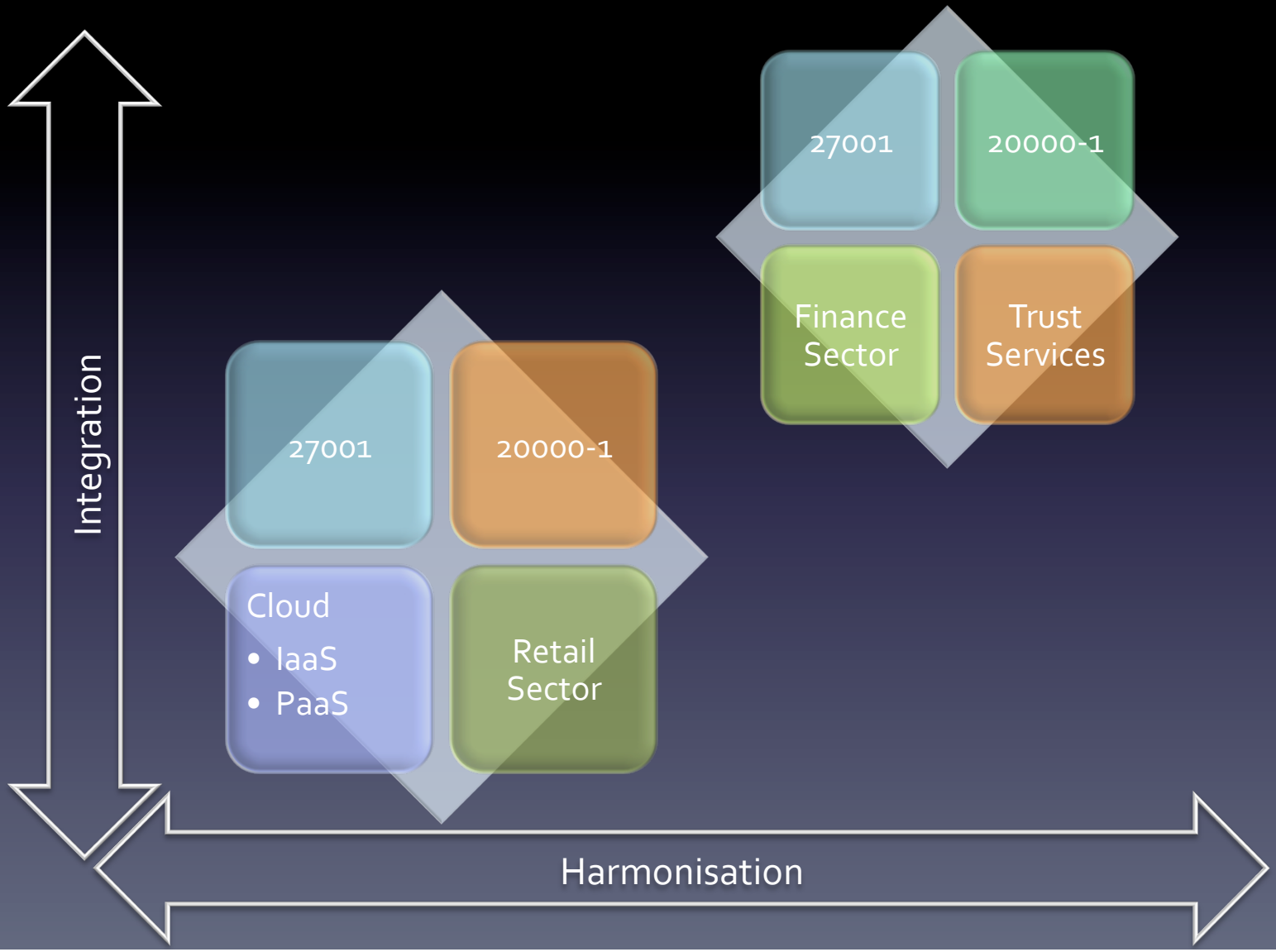
IPA

Example Integrated Management System Environment (IT Services Sector)

Some operational benefits: integrated – risk management and impact assessment, incident handling, asset management …

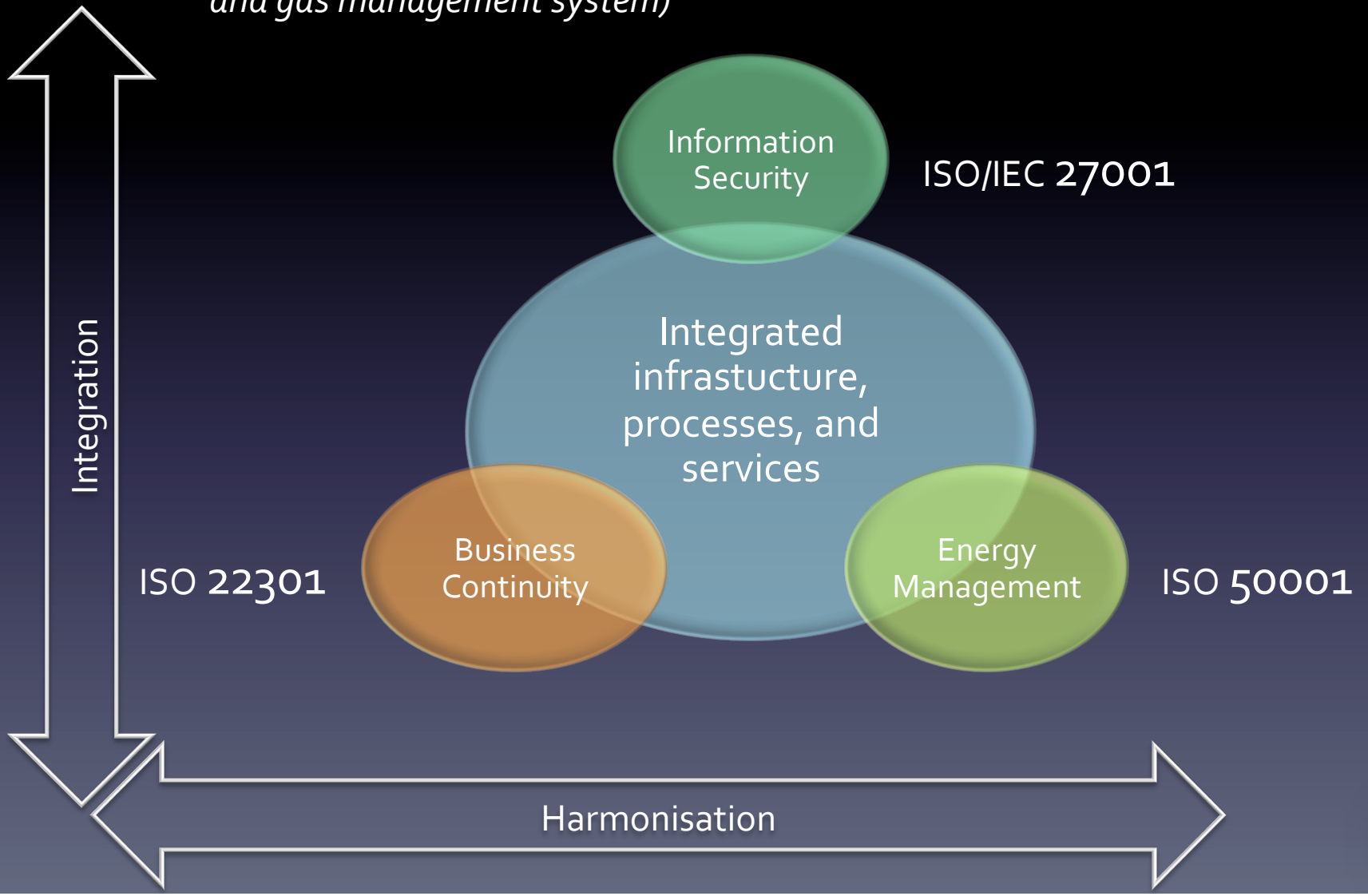


Example Integrated Management System Environment (IT Services Sector)



Example Integrated Management System Environment (IT Services Sector)

And for the Oil and Gas Industry possibly also integrated with ISO 29001 (oil and gas management system)



Highlights of the Revised 27001

- *ISO/IEC 27001 has been re-structured and aligned with the specification for the Next Generation of Management System Standards*
  - High-level structure
  - Identical core text
  - Common terms and core definitions

ISO/IEC JTC 1/SC 27 N11905
Date: 2012-11-07

ISO/IEC DIS 27001

ISO/IEC JTC 1/SC 27/WG 1

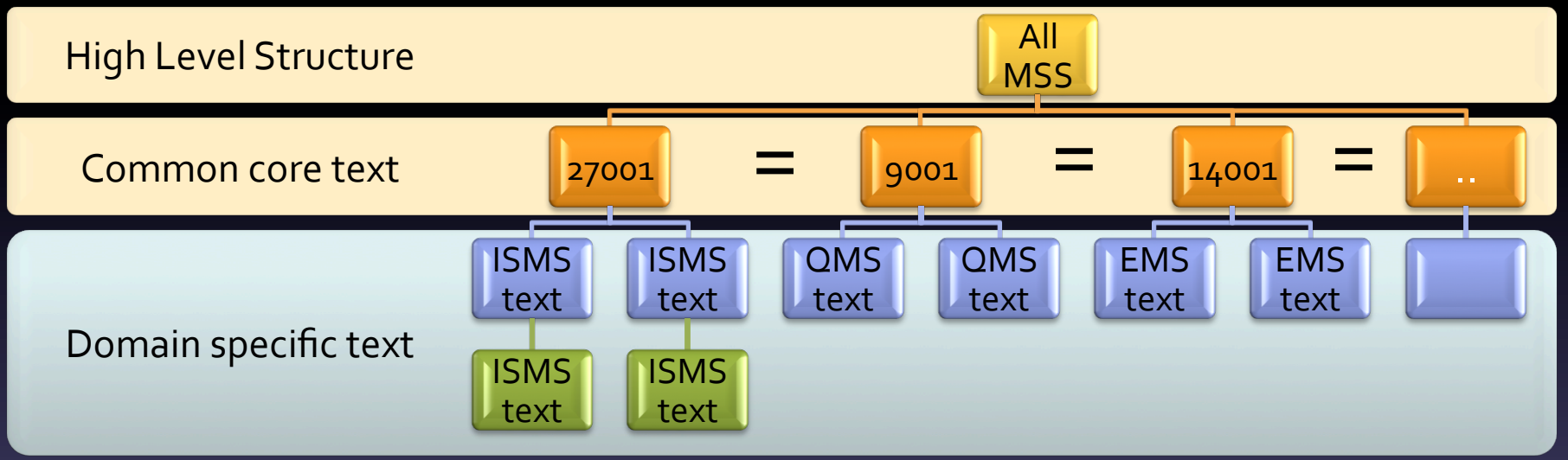
Secretariat: DIN

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité

IPA

Revised 27001 and Harmonisation



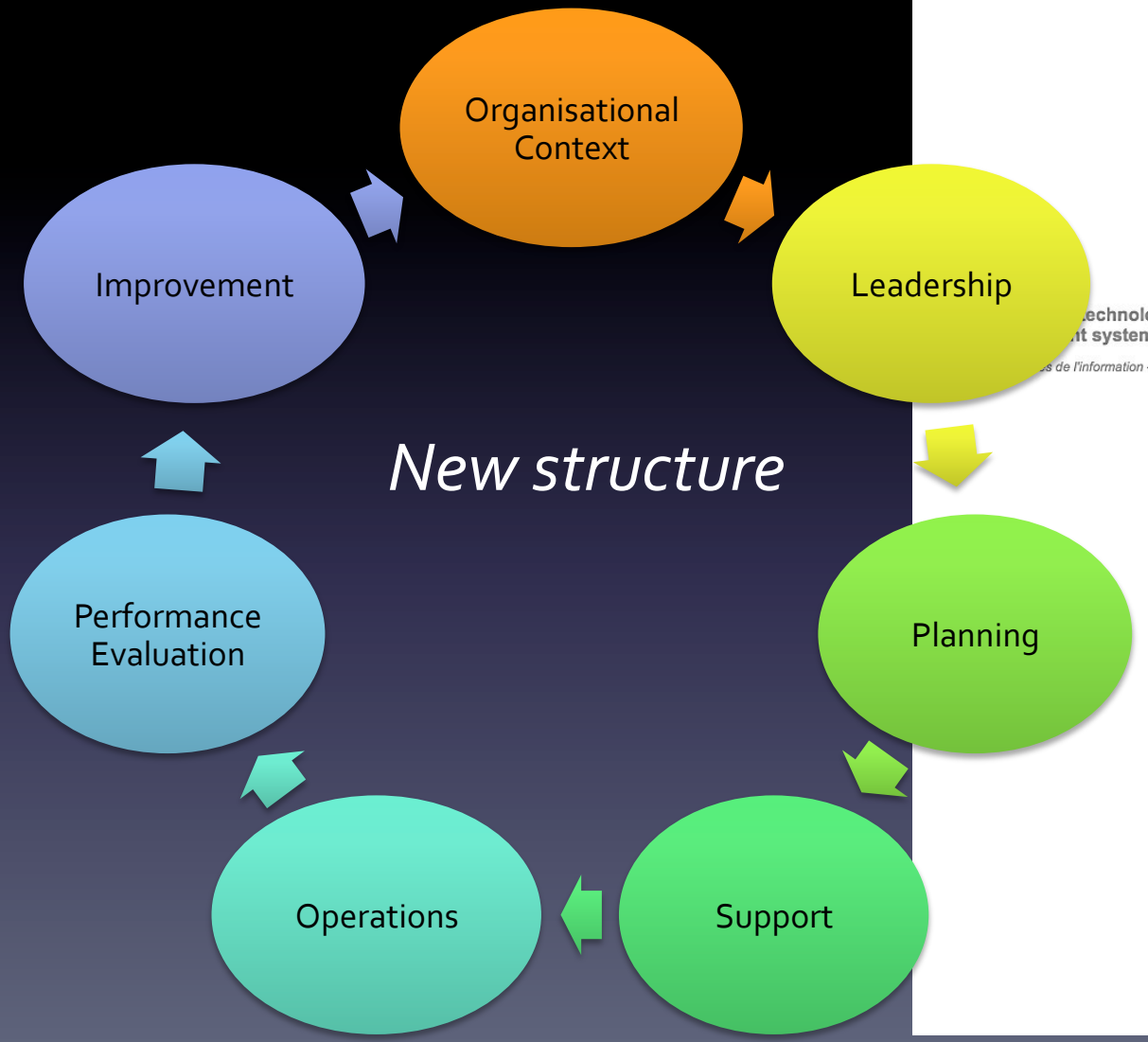
Harmonised text

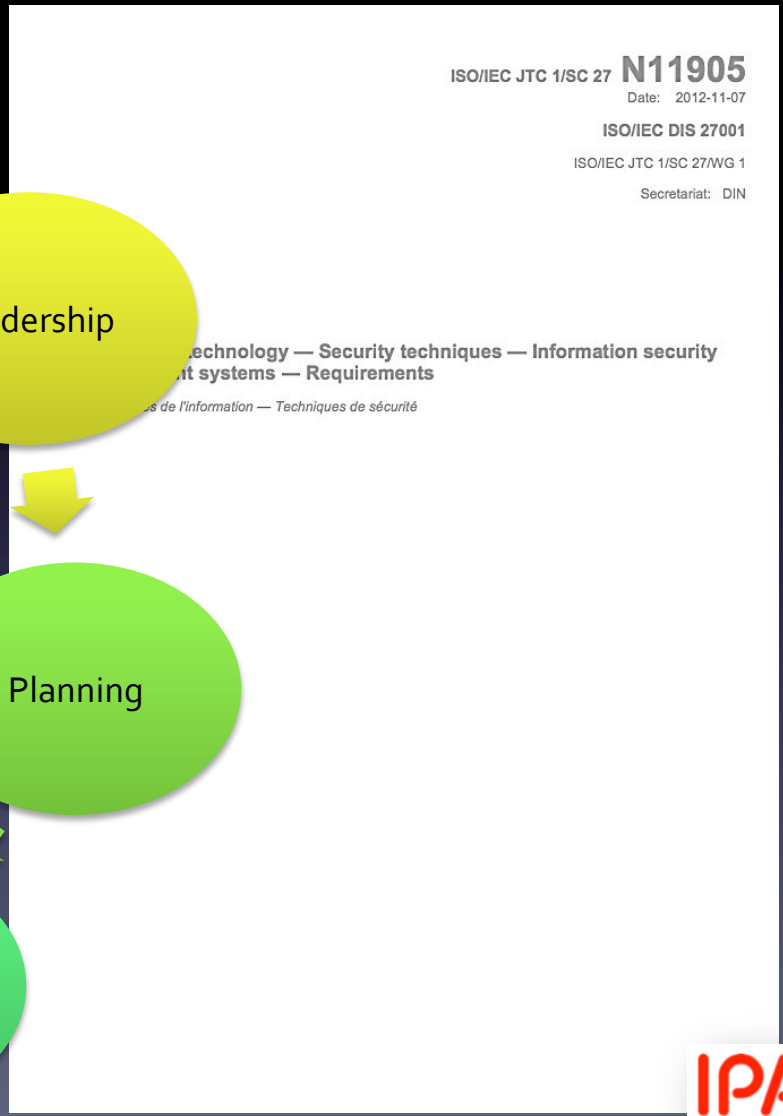
Domain specific text

Integrated and harmonised solutions

IPA

Highlights of the Revised 27001

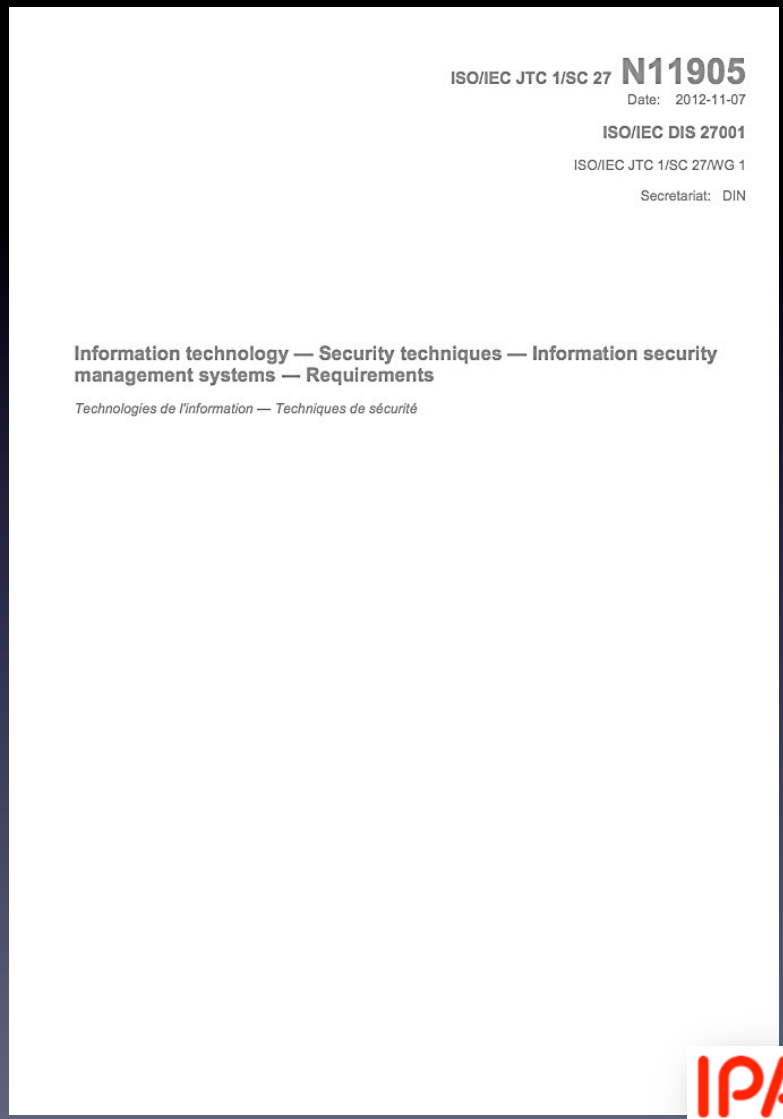



ISO/IEC JTC 1/SC 27 N11905
Date: 2012-11-07
ISO/IEC DIS 27001
ISO/IEC JTC 1/SC 27/WG 1
Secretariat: DIN
echnology — Security techniques — Information security
t systems — Requirements
s de l'information — Techniques de sécurité

IPA

Highlights of the Revised 27001

- *Improvements have been made in the areas of*
  - *Business focus*
  - *Management commitment (leadership and support)*
  - *Designing the ISMS (planning)*
  - *Deploying the ISMS (operations)*
  - *Monitoring and Reviewing the ISMS (performance evaluation)*



ISO/IEC JTC 1/SC 27 **N11905**
Date: 2012-11-07

ISO/IEC DIS 27001

ISO/IEC JTC 1/SC 27/WG 1

Secretariat: DIN

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité

IPA

Highlights of the Revised 27001

- *Risk management process has undergone several improvements and has been aligned with ISO 31000 (risk management standard)*
- *New requirements have been added based on user feedback and experiences, and some existing requirements have been modified or deleted*

ISO/IEC JTC 1/SC 27 **N11905**
Date: 2012-11-07

ISO/IEC DIS 27001

ISO/IEC JTC 1/SC 27/WG 1

Secretariat: DIN

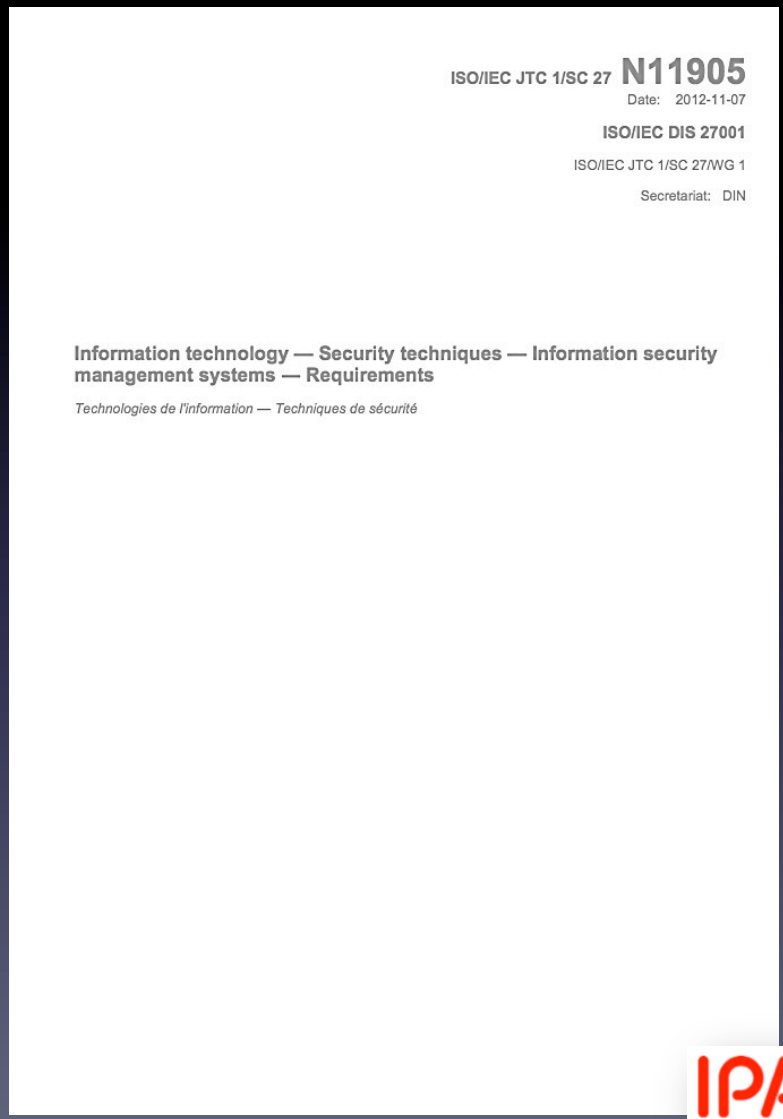
Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité

IPA

Highlights of the Revised 27001

- *New security controls and improvements of existing security controls have been made (Annex A) – parallel revision of ISO/IEC 27002 (to be released in Nov 2013)*
- *Overall the New Edition of 27001 will add more value and greater economic opportunities to the business community*



ISO/IEC JTC 1/SC 27 **N11905**
Date: 2012-11-07

ISO/IEC DIS 27001

ISO/IEC JTC 1/SC 27/WG 1

Secretariat: DIN

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité

IPA

Revision of ISO/IEC **27002**
Code of practice for information security

- Revised version has 113+ controls, as opposed to the original 133 in the 2005 version and 14 Chapter headings, rather than the original eleven Chapter headings
- Controls
  - Many controls are unchanged from the 2005 version but the implementation guidance text has been updated.
  - Some controls have been deleted since they are no longer relevant to today's interconnected world.
  - Other controls have been merged together as there was some duplication of meaning
- **Annex A of 27001** contains the control objectives and controls of this new edition of 27002
- Expected to be published Nov 2013

IPA

Success of ISO/IEC 27001 as the global **international certification standard**

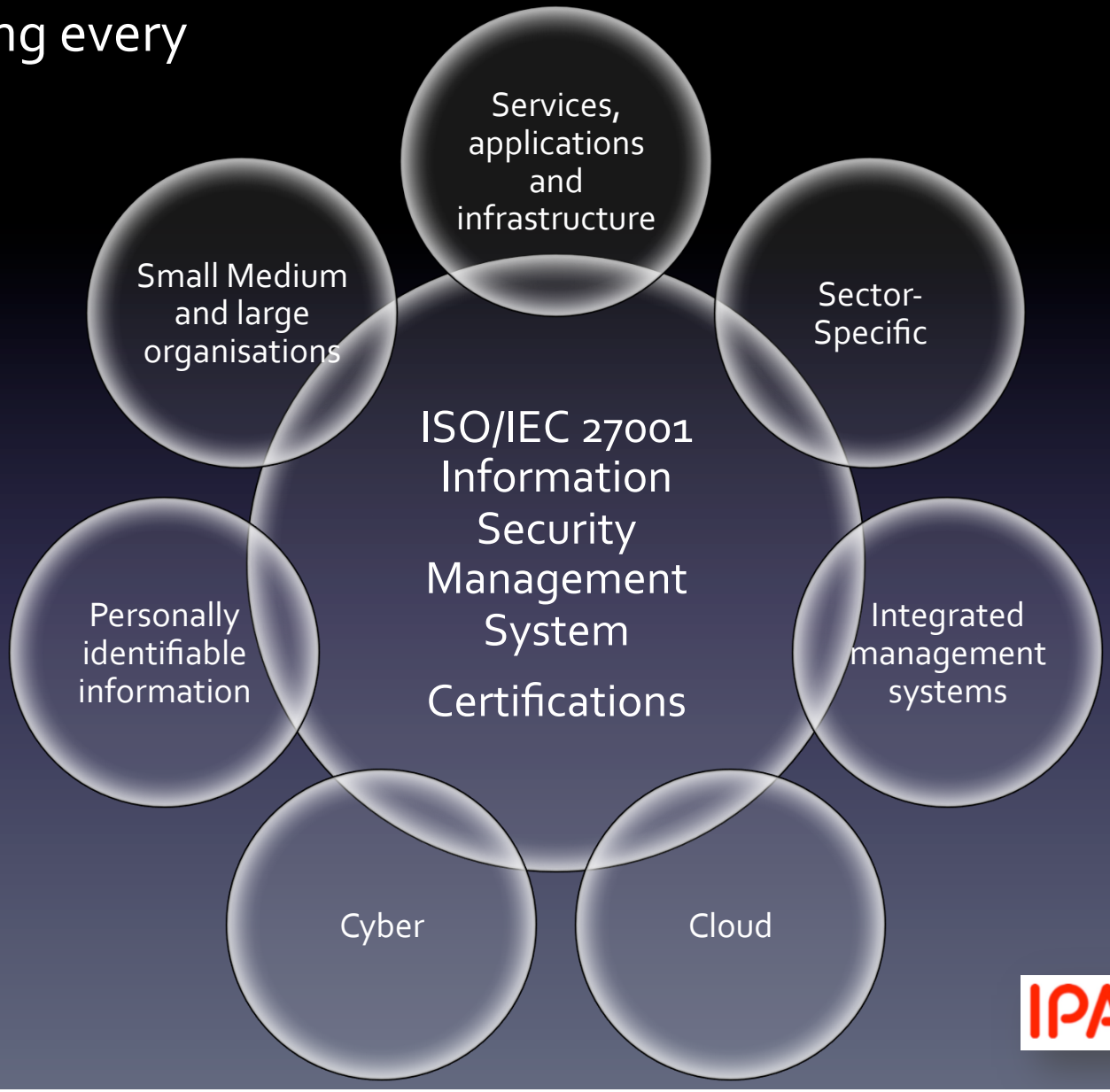
The biggest selling of all information security management standard (over 1 million of copies sold)

The international Common Language for information security management as spoken across the business world (including government use)

The international certification standard as used by the business world

IPA

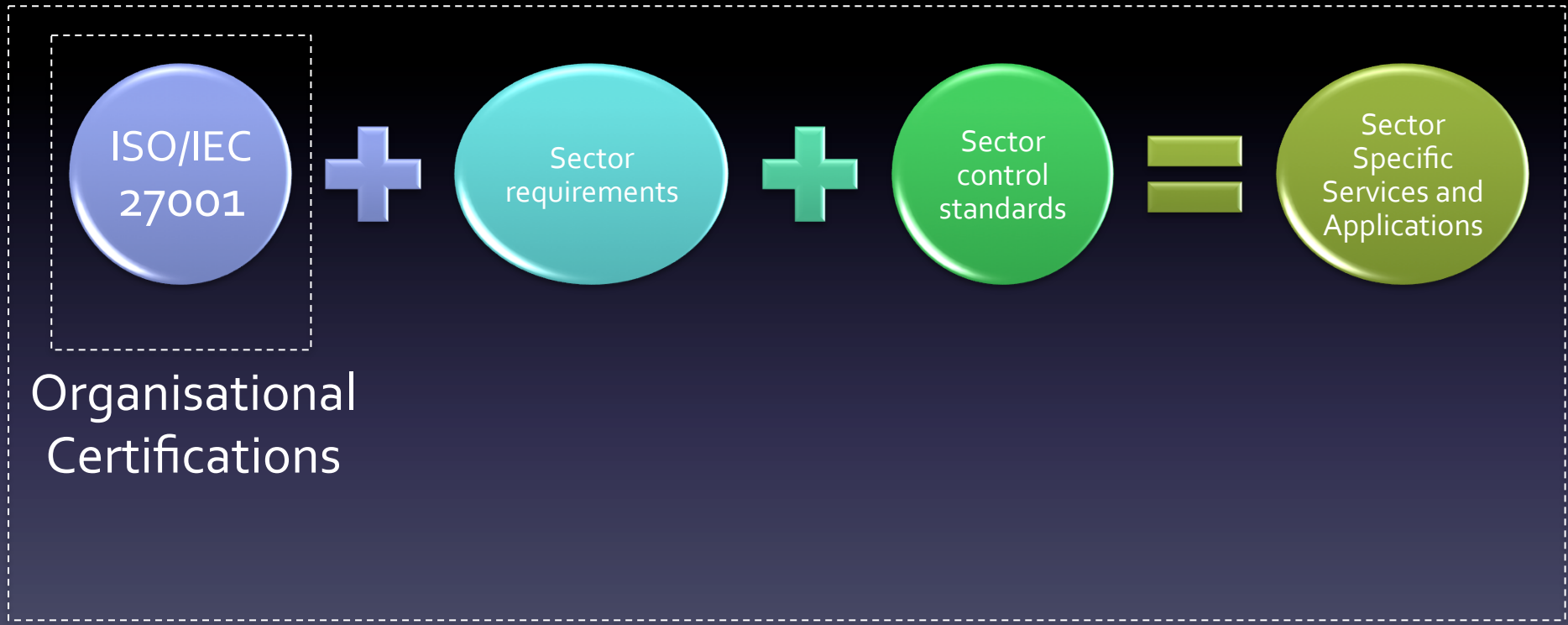
The current number of 27001 3rd party certifications is 14,000+ across 100 countries and covering every market sector



Time-Line

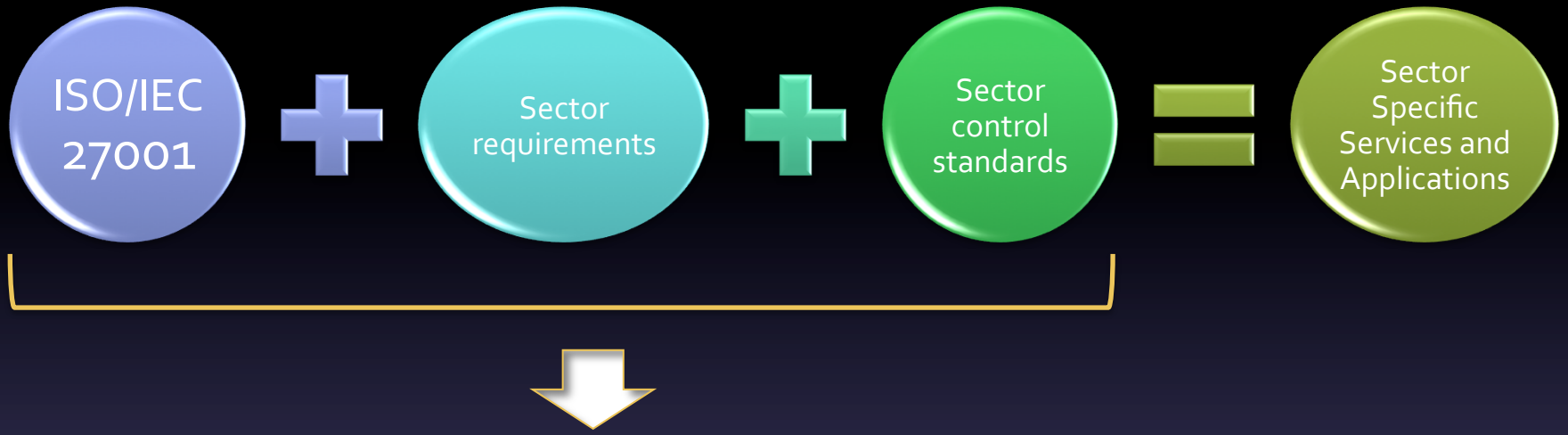

NOW
Expected Publication
Transition Deadline
May 2013
Oct/Nov 2013
Nov 2015
FDIS ballot
IS (international standard)
Two-year certification transition period

ISO/IEC 27009
Use of 27001 for Sector-Specific Applications



IPA

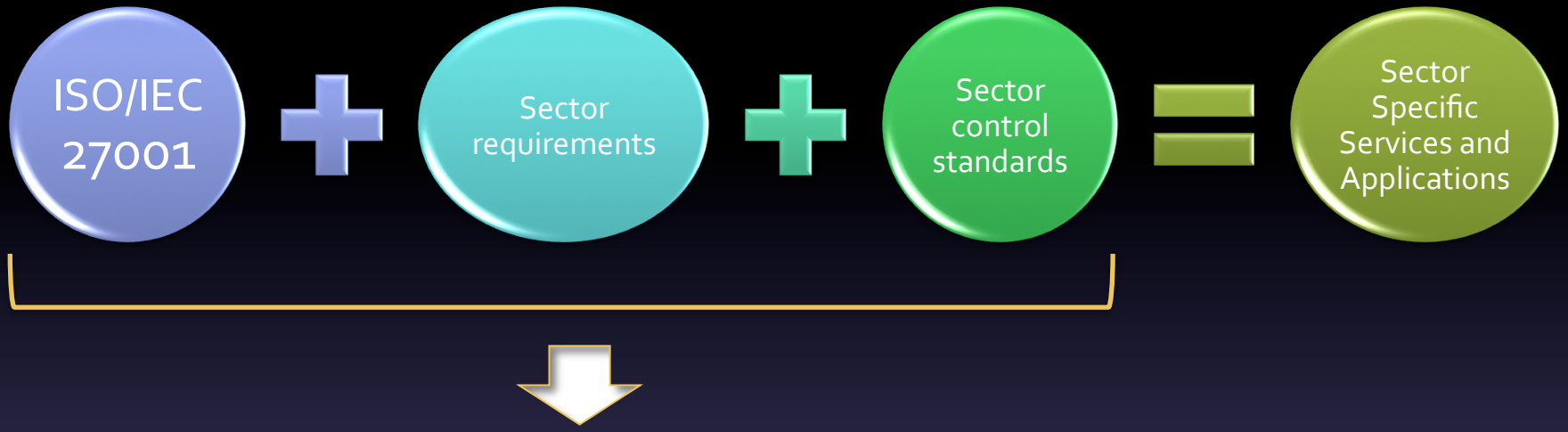
ISO/IEC 27009
Use of 27001 for Sector-Specific Applications



- *Telecoms (ISO/IEC 27011)*
- *Finance (ISO/IEC 27015 & ISO 13569)*
- *Healthcare (ISO 27799)*
- *Cyber-security (ISO/IEC 27031 +)*
- *Cloud (ISO/IEC 27017 & 27018)*
- *Industrial Control Systems*
- *Network Security Services (ISO/IEC 27033)*
- *ICT Readiness for Business Continuity (ISO/IEC 27031) and Incident Handling Services (ISO/IEC 27034)*
- *Disaster Recovery Services (ISO/IEC 24762)*
- *Supplier Relationships (ISO/IEC 27036)*
- *PII (ISO/IEC 29100 +)*

IPA

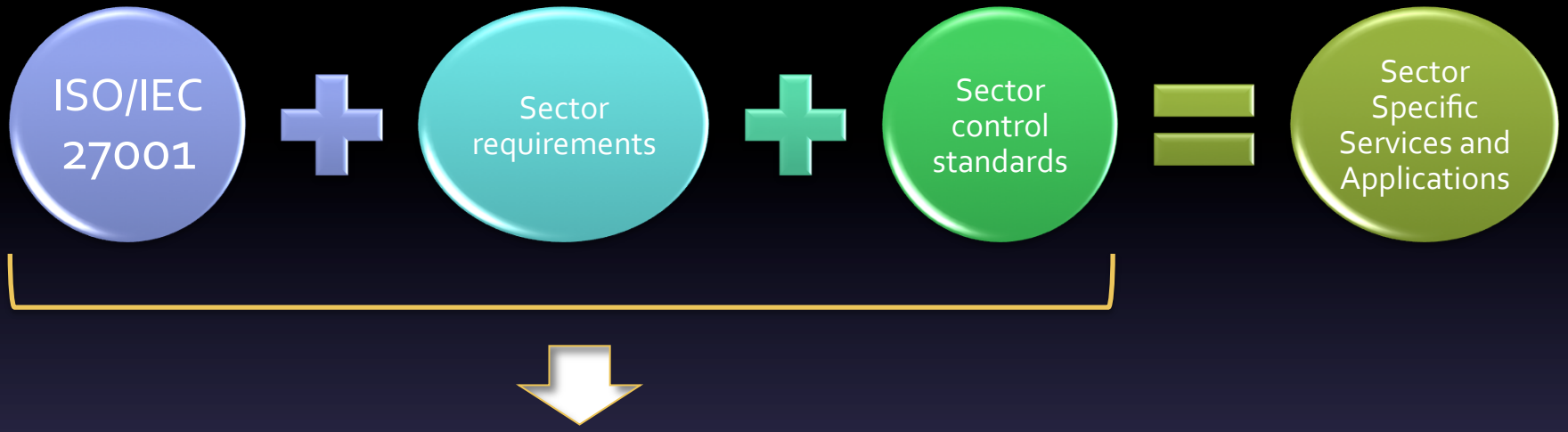
ISO/IEC 27009
Use of 27001 for Sector-Specific Applications



Telecoms certifications

- *Telecoms sector standard (X.1051 | ISO/IEC 27011)*
- *Plus other ITU-T control standards where necessary and appropriate*

ISO/IEC 27009
Use of 27001 for Sector-Specific Applications

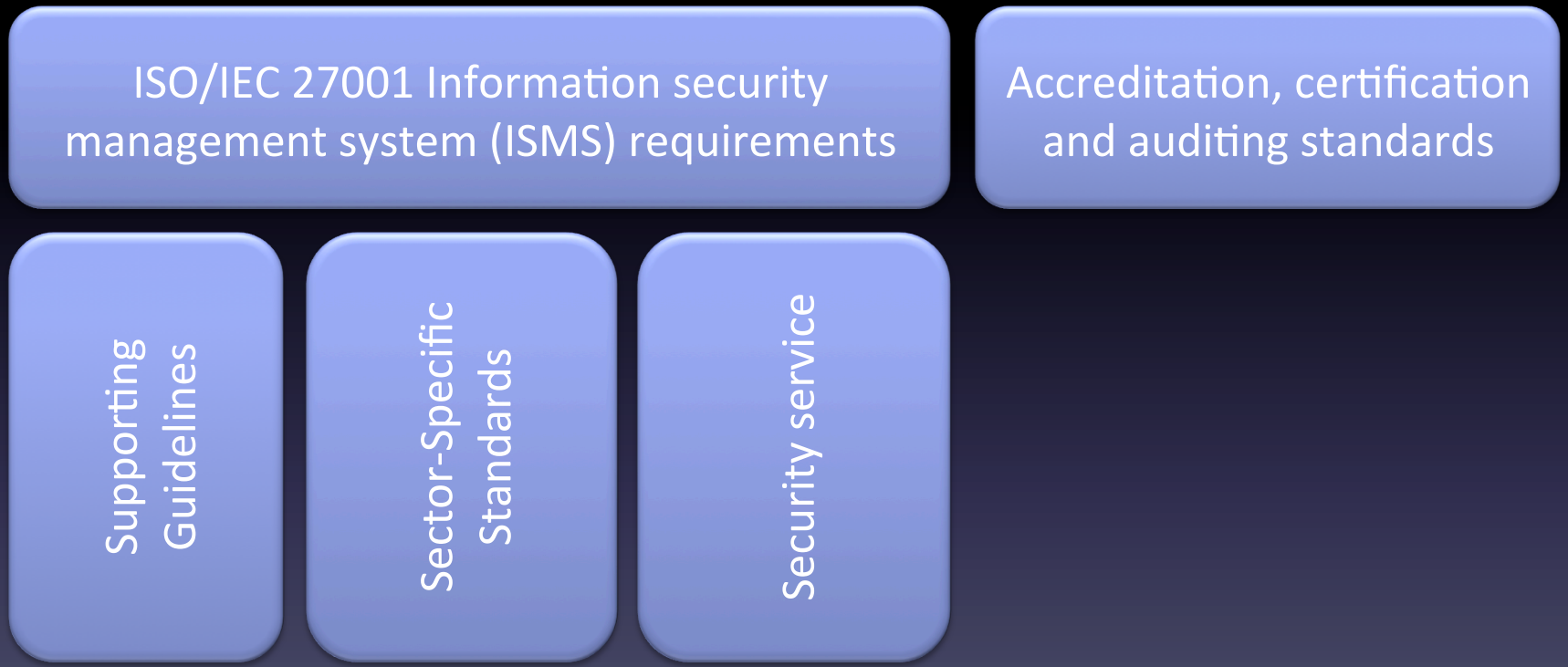


Cloud certifications

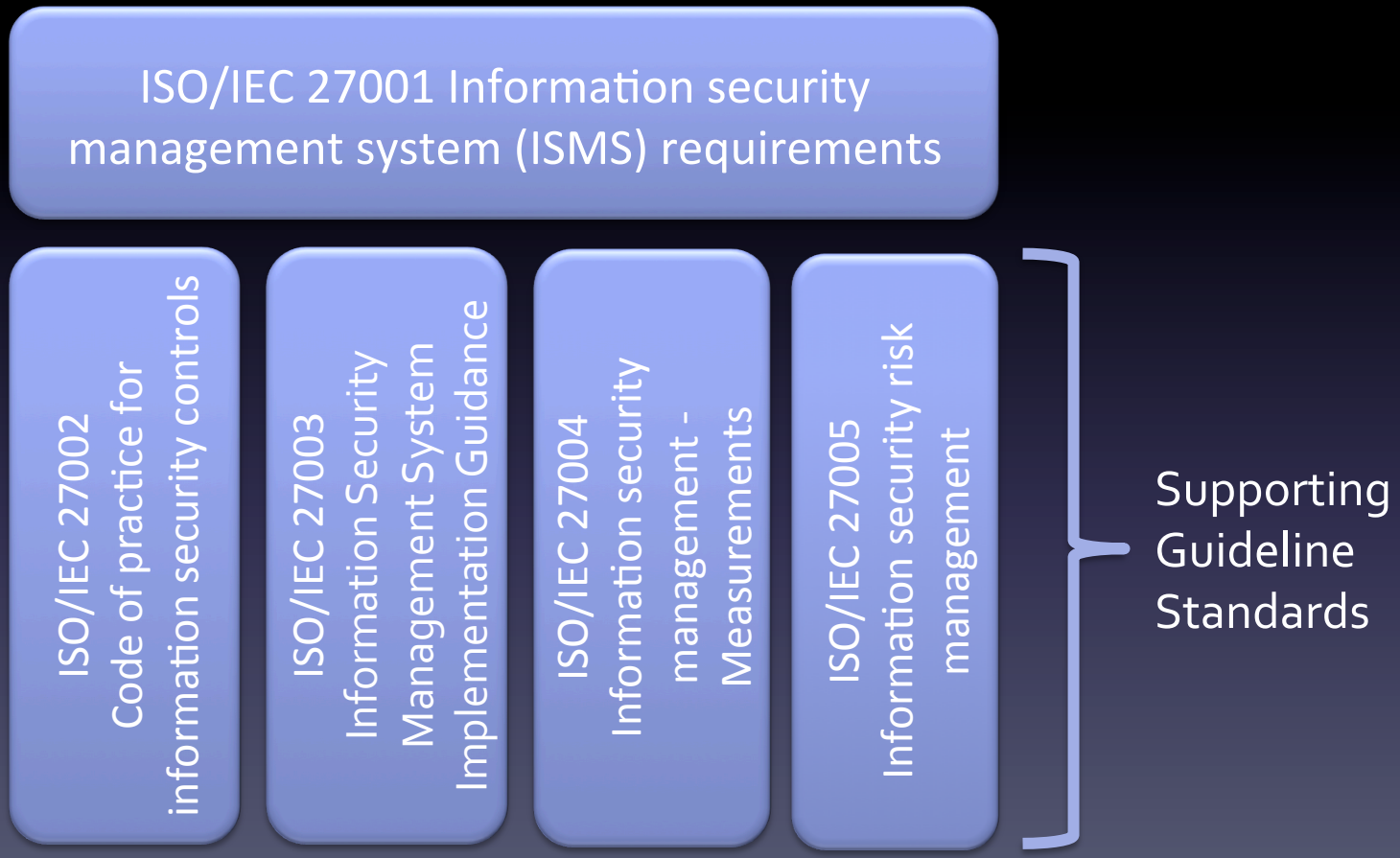
- *Code of practice for information security controls for cloud computing services based on ISO/IEC 27002 (ISO/IEC 27017)*
- *Protection of personally identifiable information (PII) (ISO/IEC 27018)*

IPA

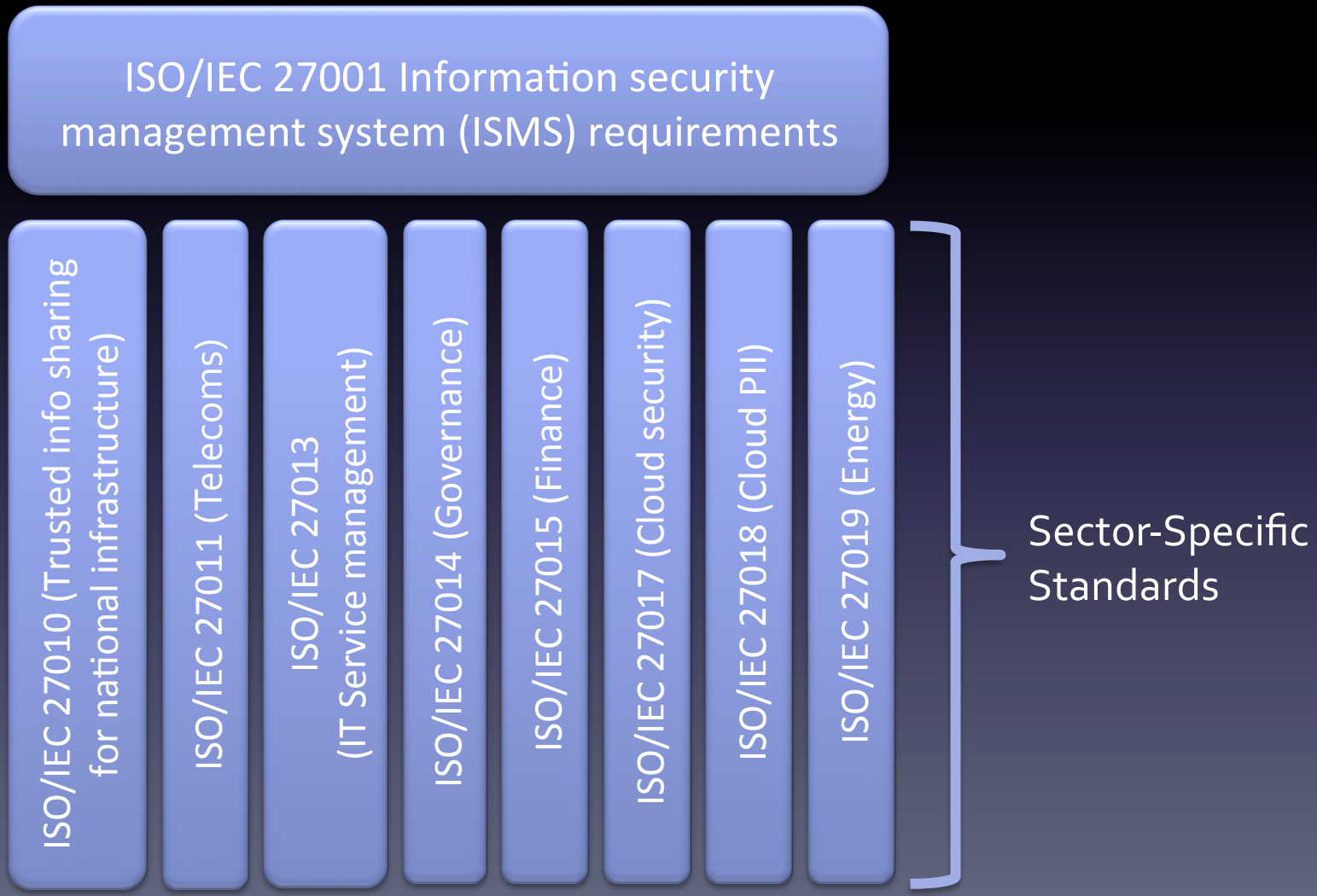
ISO/IEC 27000 Family



ISO/IEC 27000 Family Supporting Guidance

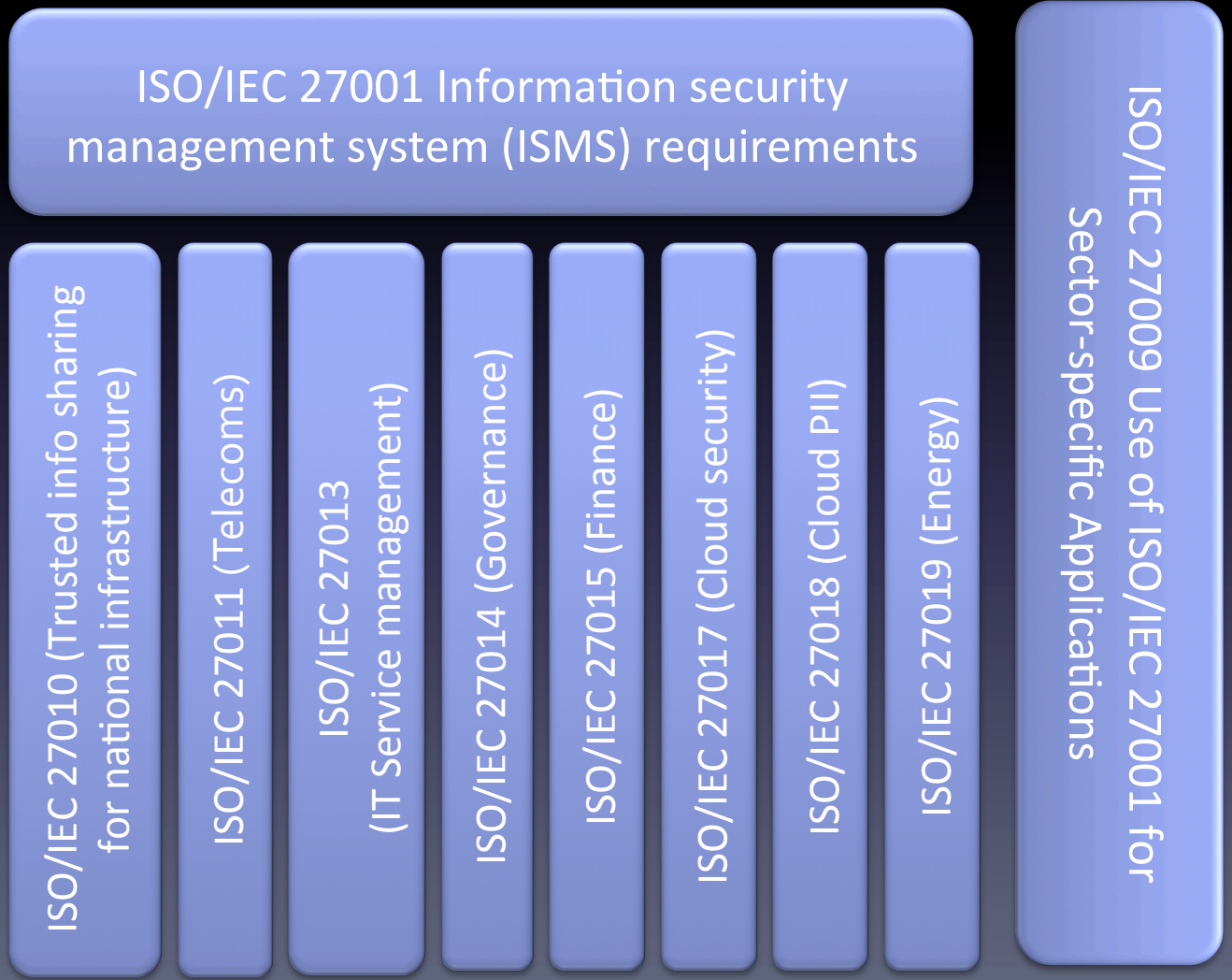


ISO/IEC 27000 Family Sector Standards



IPA

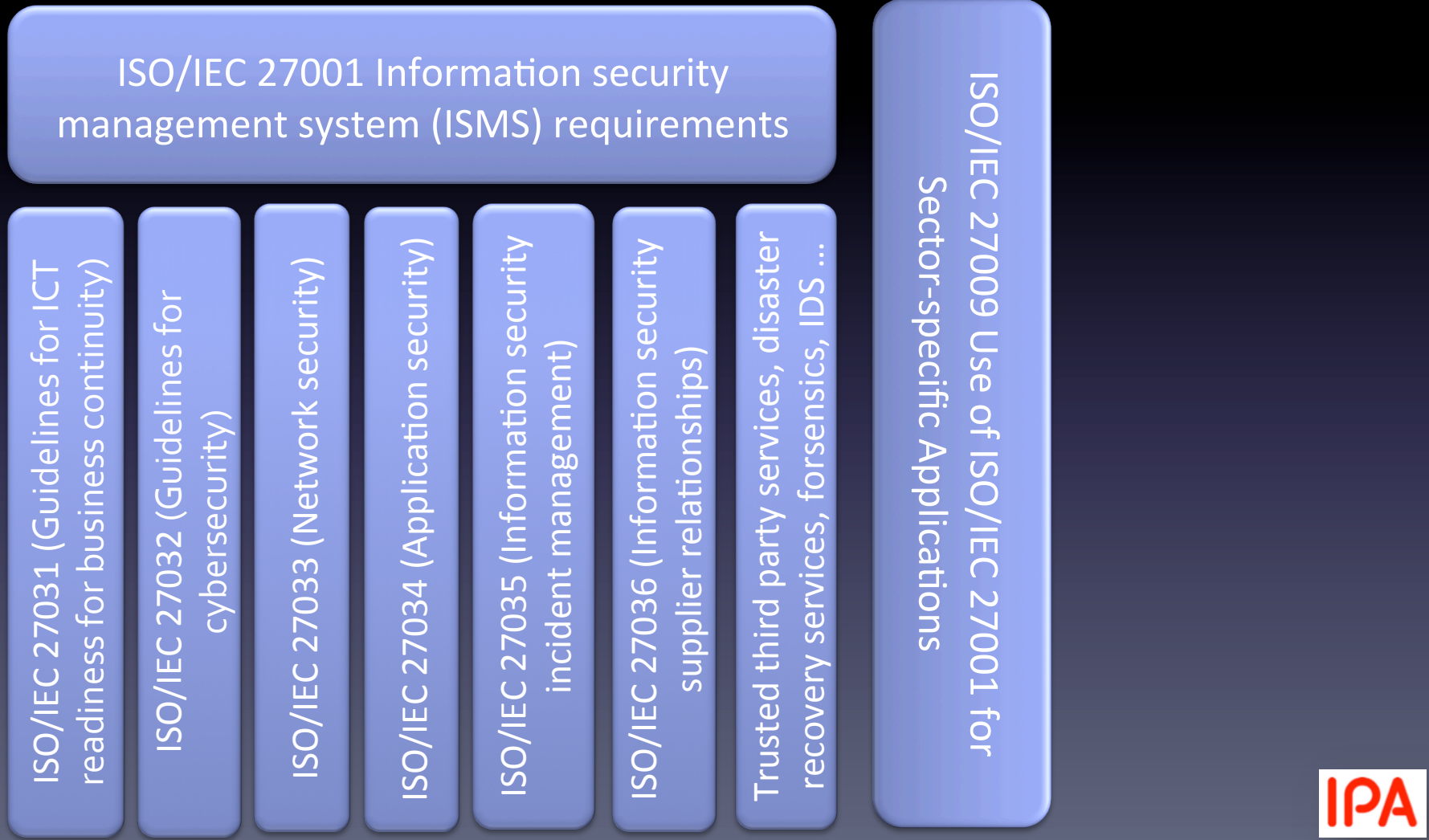
ISO/IEC 27000 Family
Sector certifications



Sector-Specific Certification

IPA

ISO/IEC 27000 Family
Services and service certifications



IPA

Some Other Developments

ISO/IEC 29100 (Privacy)

Protection of personally identifiable information *(New)*

ISO/IEC 24760 (Identity management)

ISO/IEC 27021 *(New)*

- Requirements for the Certification of Information Security Management Professionals

Study Group on IoT (Internet of Things) *(New)*

IPA

Cyber-Risks

"Forewarned is forearmed; to be prepared is half the victory." Miguel de Cervantes

let ISO/IEC 27001 help your organisation with your cyber-risks

Thanks For Listening

Prof. Edward (Ted) Humphreys

IPA Global Symposium 2013

23rd May 2013, Tokyo, Japan

IPA