LAW FORUM
ON DATA PROTECTION
& PRIVACY

GDPR General Remarks

Kostas Papadatos

MSc Infosec, CISSP-ISSMP, CISM,
ISO27001 LA, ISO27005 RM, PMP, MBCI

(ISC)² Hellenic Chapter

Founder/President

LAW FORUM ON DATA PROTECTION & PRIVACY, Friday17 February 2017, N.J.V. Athens Plaza

About… (ISC)²

INSPIRING A SAFE AND SECURE CYBER WORLD®

- (ISC)² = *International Information Systems Security Certification Consortium*
- Established in 1989
- Non-profit consortium of information security industry leaders
- Supports security professionals throughout their careers
- Global Standard for information security: (ISC)² CBK®
- Over 100,000 certified professionals; over 160 countries

- Official (ISC)2 Chapter (No: 128), 8/7/2014
- Non-Profit Association (No: 30693), 24/6/2015
- Our Mission:
  - *Exchange of ideas and dissemination of knowledge among (ISC)2 members, information security professionals and the public, as well as the promotion (ISC)2 Certifications in the region.*
- Members: **Information Security Professionals** and **(ISC)² credentialed.**

(ISC)² CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP

Regulation: IT measures as a legal tool

- **Personal data Breach = breach of security**

*"means **a breach of security** leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"*

- **Appropriate security = data processing rule**

"Data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')".

- **Data protection by design/by default**
- **Seals – Certifications and Codes of Conduct**
- **DPIAs**
- **Appointment of a DPO (Υπεύθυνος για τα Προσωπικά Δεδομένα)**
- **Data Breach Reporting – Implementation of Robust Security Measures**

Privacy vs Security

Information (Data) Security

- Covers **Confidentiality, Integrity and Availability** of **ALL Critical Data**.
- Ensures that data is accurate and available when those **with authorized access need it**.
- Data can be **highly secured while violating privacy principles**.
- Information-security practitioners often don't understand the human side of privacy.

Data Privacy

- is suitably defined as the **Appropriate Use** of **Personal Data**.
- Governs how information pertaining to individuals is **collected, processed and protected**.
- Privacy has a very human face, and unlike information-security controls, is **less measurable**.
- Privacy professionals may not always understand the implementation of technology controls.

Privacy of electronic information would not be possible without security safeguards (appropriate people, policies, process and technology).

Typical Security Controls

Organizational Controls

People

- Training
- Awareness
- HR Policies
- Background Checks
- Define Roles
- Responsibilities
- Performance Management …

Policies / Procedures

- Risk Assessment
- Asset Management
- Data Classification
- User Access Management
- Access Management
- Change Management
- Patch Management
- Configuration Mgmt
- Incident Response
- Business Continuity
- Legal & Regulatory Compliance
- Secure SDLC …

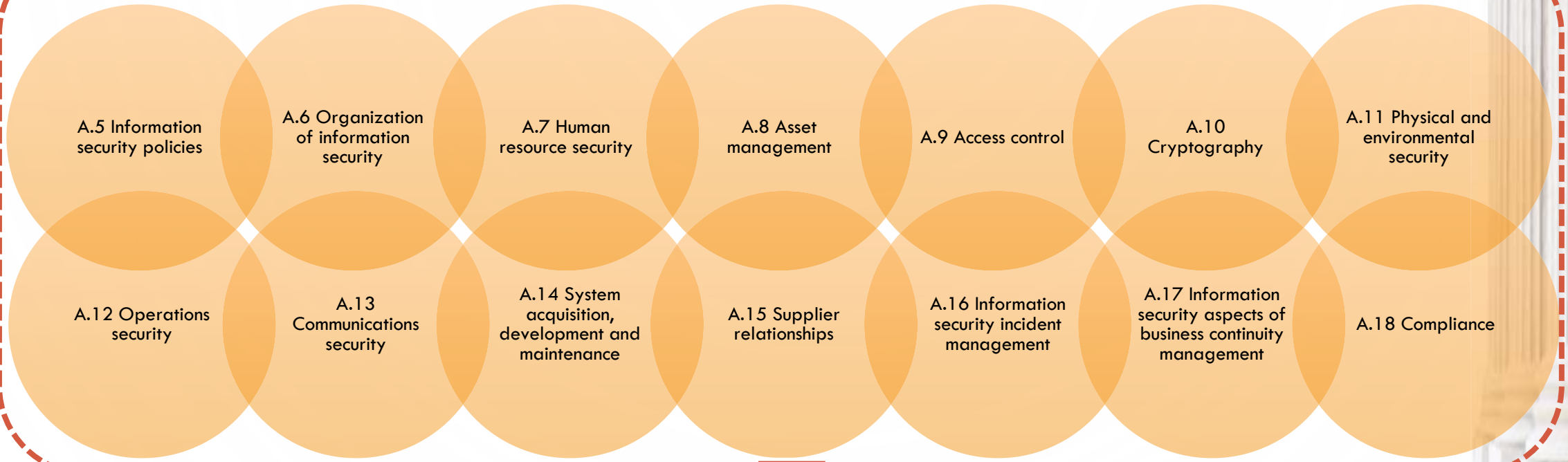
Technology (Products)

- Physical Security
- UTM. Firewalls
- System Security (FIM)
- IDS/IPS
- Web Content Security
- Email Content Security
- Vulnerability Assessment
- Penetration Testing
- Web Application Firewall
- DB Firewall
- Log Management/SIEM
- Managed Services & Cyber Intelligence
- Data Leak Prevention
- Data Classification
- Identity Management
- Encryption (DB, File, Mail, VPNs …)
- Patch Management
- WiFi Security
- Mobile Device Management
- APTs Defense
- Password Management
- Antivirus …

Beware of Security Controls conflicting with Privacy (e.g. DLP) !

"State of the Art" … "Standards" and "Best Practices"?

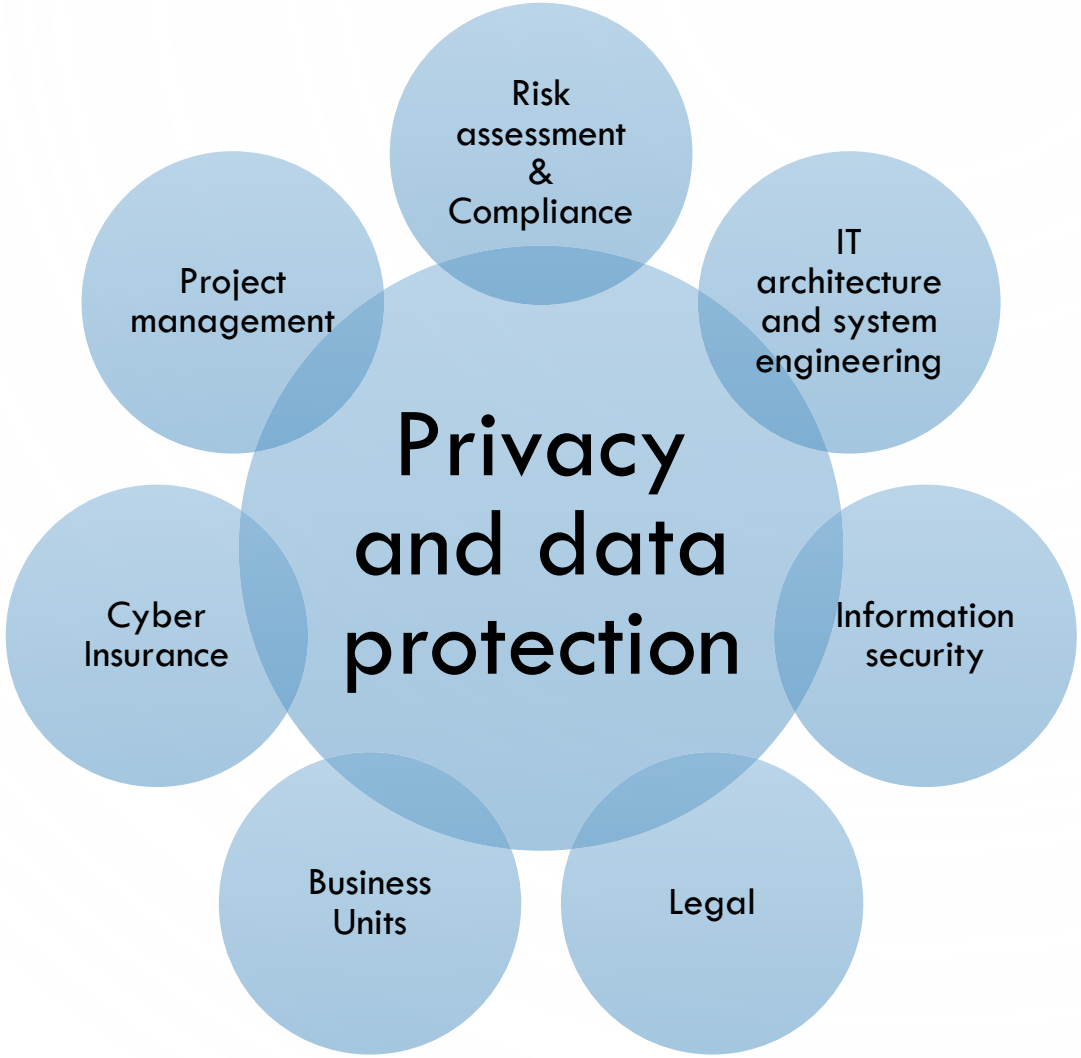
ISO 27001: Annex A Domains



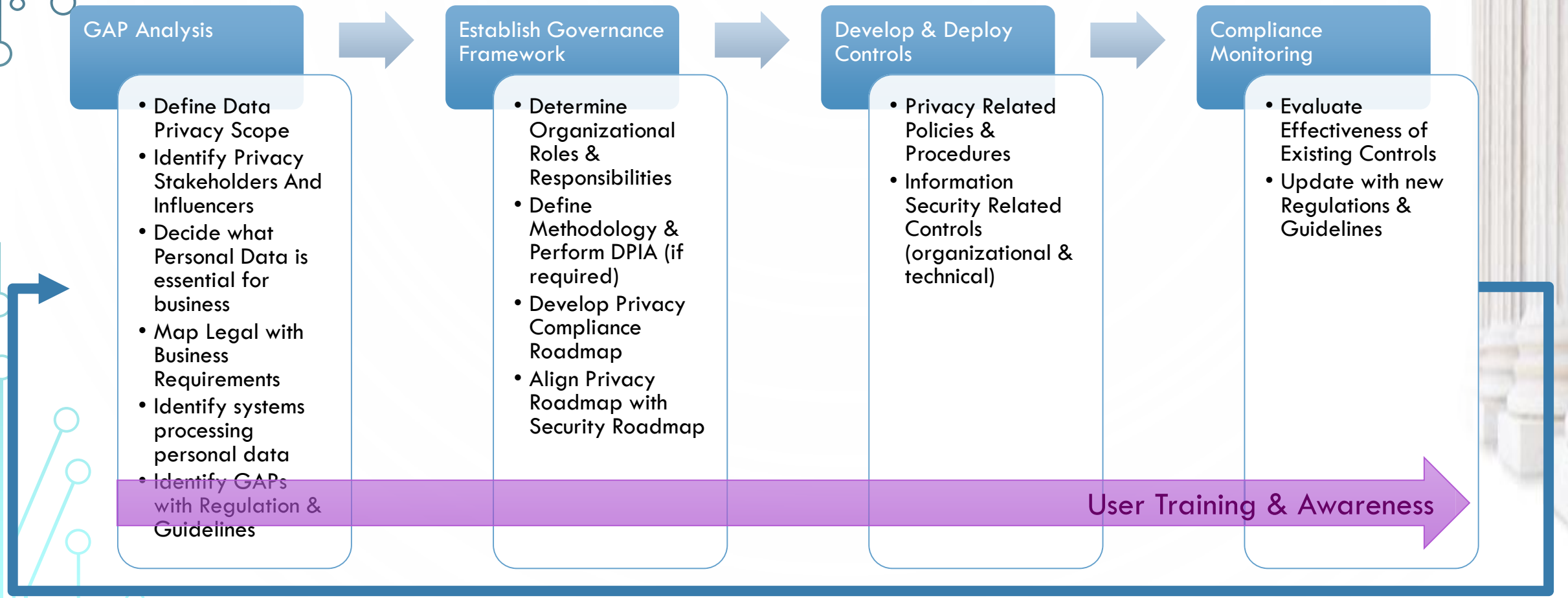
ISO 27018:

Code of practice *for protection of personally identifiable information (PII) in public clouds acting as PII processors.*

Multidisciplinary Team & Combined Expertise



Overall Compliance Strategy



Thank You!