Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Centre for Information Policy Leadership (CIPL) Webinar on ISO 27701 and CIPL's Accountability Framework

29 January 2020

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Speakers

Nathalie Laneret

Director of Privacy Policy, CIPL

NLaneret@HuntonAK.com

Brian Philbrook

Privacy Counsel, OneTrust

BPhilbrook@OneTrust.com

Florian Thoma

Senior Director of Global Data Privacy, Accenture

Florian.Thoma@Accenture.com

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Agenda

- 11:30 **Introduction to Accountability and Certifications**
- 11:40 **What is ISO 27701 and what are its benefits?**
- 12:00 **Program Preparation and Getting Certified**
- 12:20 **ISO 27701 mapped to CIPL's Accountability Framework**
- 12:25 **Q&A**
- 12:30 **End of Webinar**

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Introduction to Accountability & Certifications

A Global Privacy and Security Think Tank

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

BRIDGING REGIONS | BRIDGING INDUSTRY & REGULATORS | BRIDGING PRIVACY AND DATA DRIVEN INNOVATION

ACTIVE GLOBAL REACH

85+ Member Companies

5+ Active Projects & Initiatives

20+ Events annually

15+ Principals and Advisors

We **INFORM** through publications and events

We **NETWORK** with global industry and government leaders

We **SHAPE** privacy policy, law and practice

We **CREATE** and implement best practices

ABOUT US

- The Centre for Information Policy Leadership (CIPL) is a global privacy and security think tank
- Based in Washington, DC, Brussels and London
- Founded in 2001 by leading companies and Hunton Andrews Kurth LLP
- CIPL works with industry leaders, regulatory authorities and policy makers to develop global solutions and best practices for data privacy and responsible use of data to enable the modern information age

Twitter.com/the_cipl

https://www.linkedin.com/company/centre-for-information-policy-leadership

www.informationpolicycentre.com

2200 Pennsylvania Ave NW
Washington, DC 20037

Park Atrium, Rue des Colonies 11
1000 Brussels, Belgium

30 St Mary Axe
London EC3A 8EP

Implementing Accountability

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Organizations must be able to demonstrate accountability – internally and externally

Accountability is not static, but dynamic, reiterative and a constant journey

Accountability requires comprehensive privacy programs that translate legal requirements into risk-based, verifiable and enforceable corporate practices and controls

Company values and business ethics shape accountability

Accountability – Examples of Content of Privacy Management Programs

Leadership and Oversight

- Tone from the top
- Executive oversight
- Data privacy officer/office of oversight and reporting
- Data privacy governance
- Privacy engineers
- Internal/External Ethics Committees

Risk Assessment

- At program level
- At product or service level
- DPIA for high risk processing
- Risk register
- Risk to organizations
- Risk to individuals
- Records of processing

Policies and Procedures

- Internal privacy rules based on DP principles
- Information security
- Legal basis and fair processing
- Vendor/processor management
- Procedures for response to individual rights
- Other (e.g. Marketing rules, HR rules, M&A due diligence)
- Data transfers mechanisms
- Privacy by design
- Templates and tools for PIA
- Crisis management and incident response

Transparency

- Privacy policies and notices to individuals
- Innovative transparency – dashboards, integrated in products/apps, articulate value exchange and benefits, part of customer relationship
- Information portals
- Notification of data breaches

Training and Awareness

- Mandatory corporate training
- Ad hoc and functional training
- Awareness raising campaigns and communication strategy

Monitoring and Verification

- Documentation and evidence - consent, legitimate interest and other legal bases, notices, PIA, processing agreements, breach response
- Compliance monitoring and testing - verification, self-assessments and audits
- Seals and certifications

Response and Enforcement

- Individual requests and complaints-handling
- Breach reporting, response and rectification procedures
- Managing breach notifications to individuals and regulators
- Implementing response plans to address audit reports
- Internal enforcement of non-compliance subject to local laws
- Engagement/Co-operation with DPAs

Organizations must be able to **demonstrate their own implementation** - internally and externally

Accountability – What it is and What it is not

What it is

Comprehensive
- Comprehensive internal program giving effect to DP requirements
- Verifiable, demonstrable and enforceable data protection commitment, infrastructure and controls

Relevant
- Relevant and scalable for all organizations
- Private and public sector; large multinationals and SMEs; controllers and processors

Consistent
- Consistent with other areas of corporate law and governance and duty of care
- Anti-bribery; anti-money laundering; export controls; Sarbanes-Oxley; Sustainability; Fiduciary duty

Demonstrable
- Internally: Executive leadership; Board of Directors; shareholders
- Externally: Business partners; regulators; individuals; civil society

Effective
- Corporate Digital Responsibility fit for 21st century
- Delivers effective protection for individuals and data
- Enables responsible use, sharing and flows of data and innovation

What it is not

Self Regulation
- Sits on top of and in addition to legal requirements - it does not replace them (co-regulation)
- Accountability operationalizes legal rules and delivers legal compliance

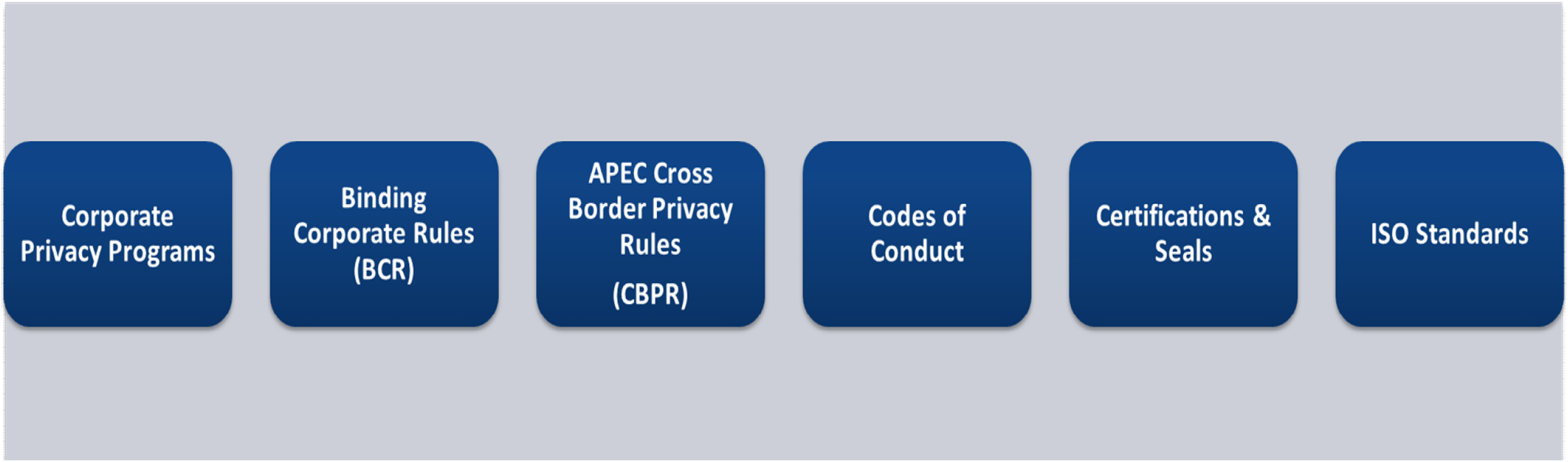
Carte Blanche to use data
- Requires organizations to implement all applicable DP norms and be able to demonstrate that implementation

Self serving tool
- Provides also benefits for regulators, individuals and society

An excuse for failure
- Minimizes the risks of breaches, and requires organizations to be prepared, responsive and responsible when they occur
- Can be a mitigating factor in enforcement, but it does not give organizations a free pass

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Examples of Privacy Management Frameworks



Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

What is ISO 27701 and what are its benefits?

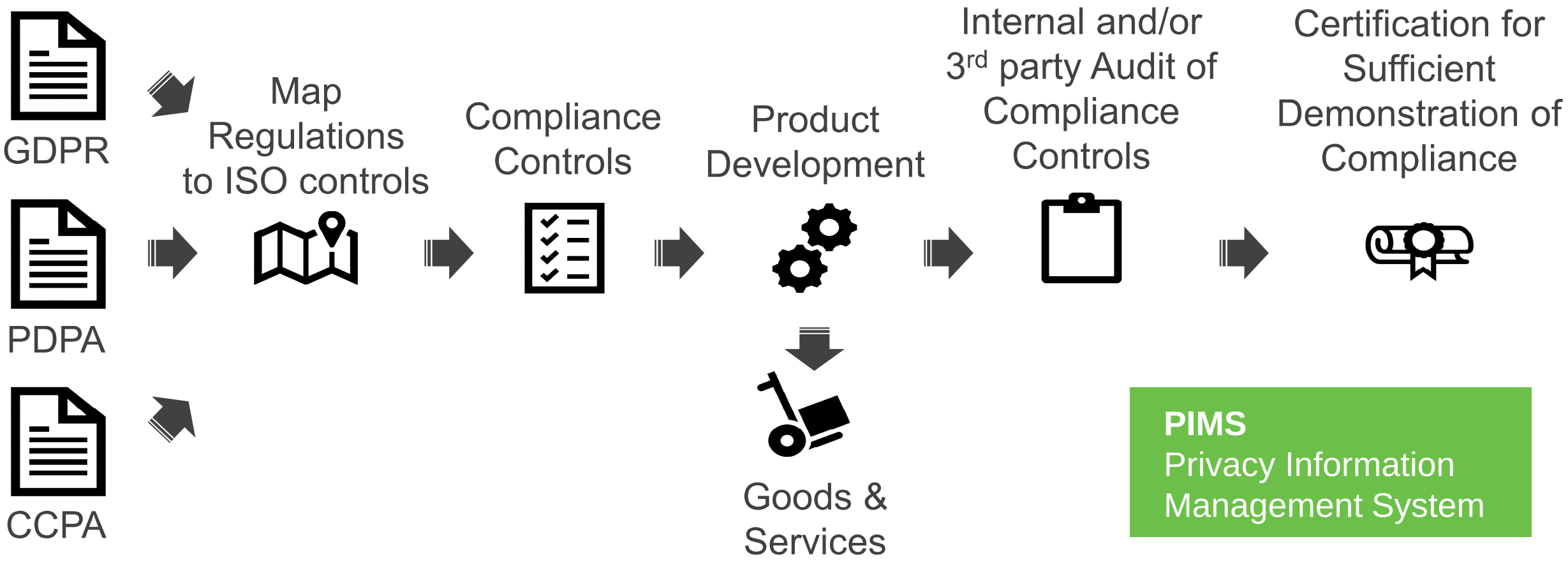
What is ISO 27001?

Privacy Information Management System (PIMS)

Privacy extension to ISO 27001	Establishing, implementing, maintaining and continually improving a PIMS in the form of an extension to ISO 27001 for privacy management within the context of the organization
PIMS-specific requirements and guidance	A privacy information management system (PIMS) expands upon the ISMS and addresses the protection of privacy as potentially affected by the processing of PII
Extended interpretation	Where "information security" is used in ISO 27001 and 27002, "information security and privacy“ applies instead

The Design Intent of ISO 27701

A universal set of operation controls to reconcile privacy regulations into practice

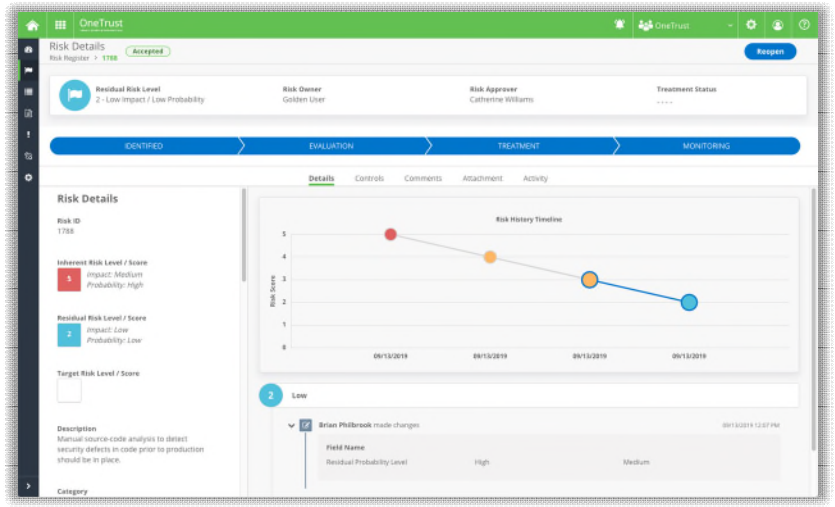


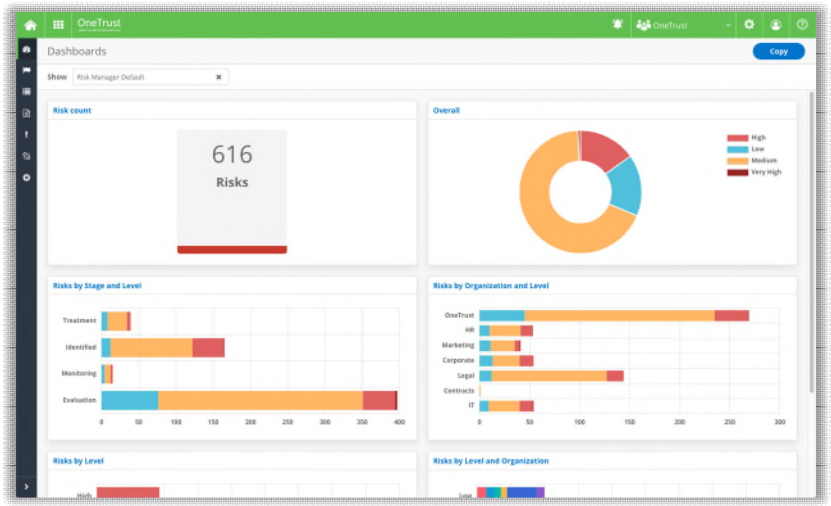
PIMS
Privacy Information Management System

OneTrust
PRIVACY, SECURITY & THIRD-PARTY RISK

Core Components

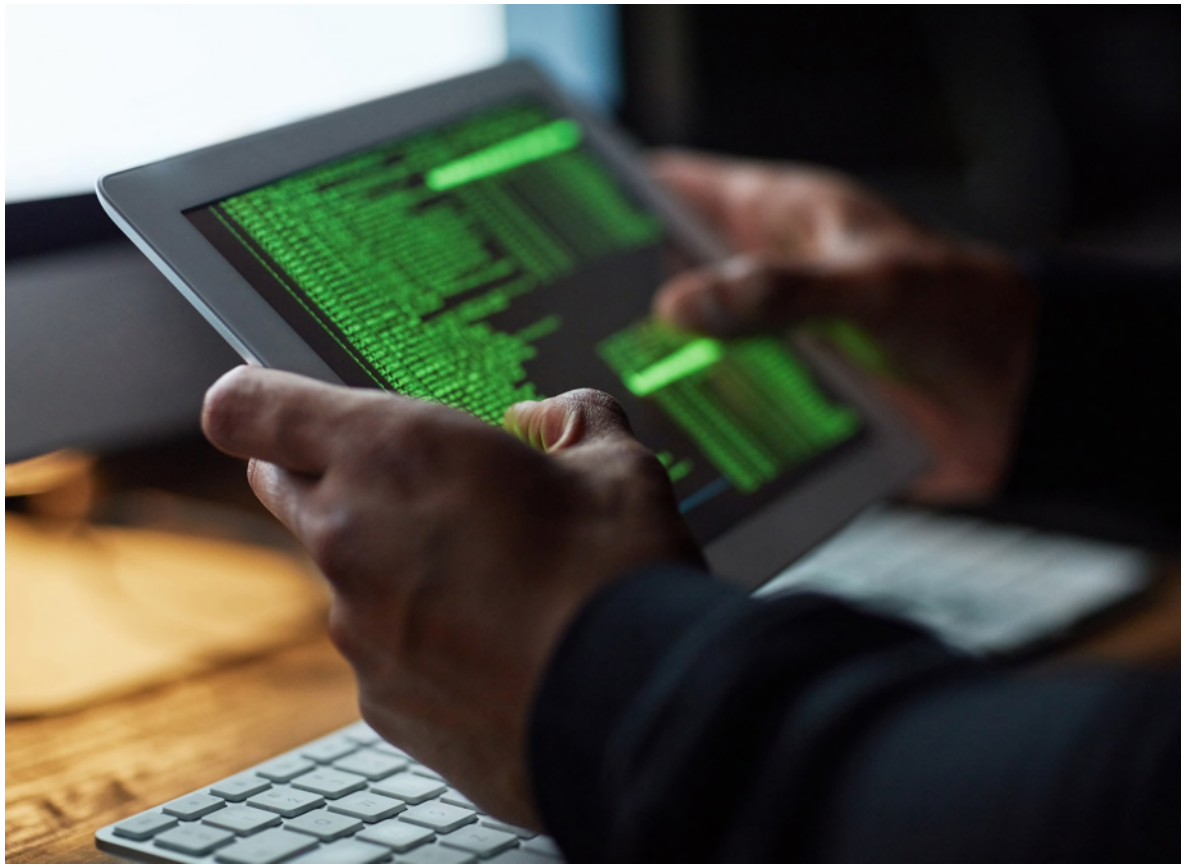
Context & Scope	Determine context or organization and scope of certification Two sets of controls: Controller and Processor
Risk Assessments	Add privacy to annual risk assessment process Identify, calculate and treat risks
Privacy Impact Assessments	Implement PIAs where appropriate New or changes to existing processing activities
Records of Processing	Maintain records of processing activities Include details such as the type and purpose of processing
Consent Management	Ensure valid consent, where applicable Record consent details and maintain evidence
Data Subject Rights	Facilitate data subject rights Meet obligations and ensure transparency
Vendor Management	Maintain DPAs with third parties Assess and track processors and sub-processors
Incident Response	Identify, track and resolve personal data breaches Add privacy breaches to incident response plan





OneTrust
PRIVACY, SECURITY & THIRD-PARTY RISK

Benefits of ISO 27701 Certification



- Build trust and provide assurance
- Demonstrate compliance
- Promote continuous improvement
- Ensure flexibility and scalability
- Reduce risk

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Program Preparation and Getting Certified

WHAT'S THE BIG DEAL?

OUR CLIENTS
Build trust and assurance for clients that Accenture protects clients' data and Accenture is in a position to help our clients do the same for their clients

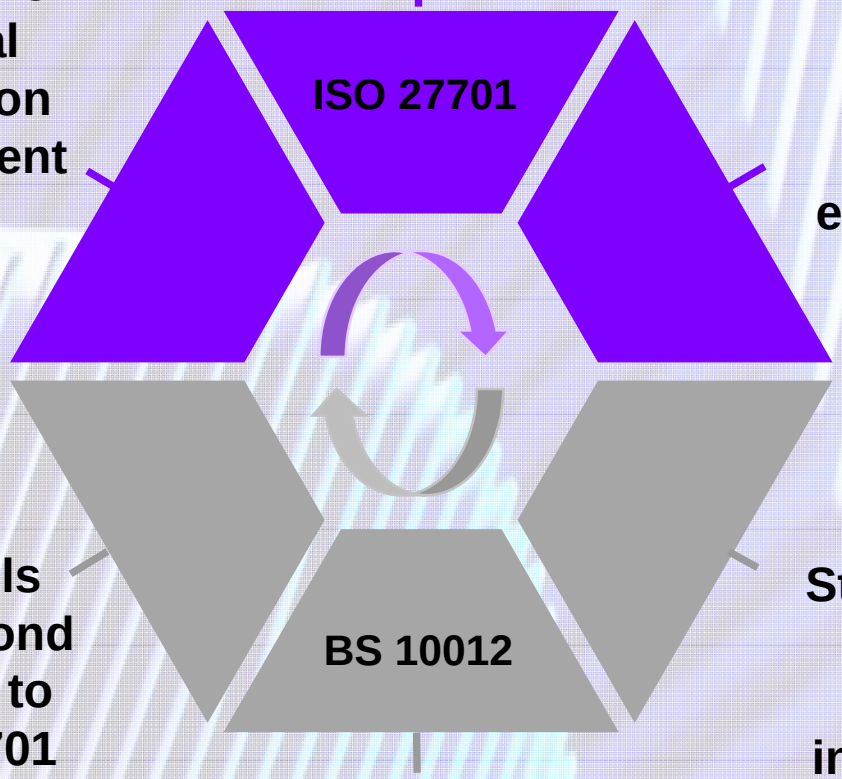
Reduce formal compliance burden on clients (e.g., need to conduct audits)

OUR PEOPLE
Demonstrate to Accenture people our commitment to protecting personal data internally and externally

OUR REGULATORS
Offer strong evidence of compliance to applicable privacy requirements to which the Standards are mapped.

FUTURE
Potential use of certifications as a transfer mechanism

ACCENTURE DATA PRIVACY CERTIFICATIONS



Certifies the personal data controllership of Accenture's enterprise

A Global Standard for personal information management

Future plans include certifying Accenture client engagement functions

Controls correspond closely to ISO 27701 Standard

A British Standard by BSI for personal information management

Certifies Accenture client engagements that process EU data globally

ISO 27701

STANDARD AND CERTIFICATION

- PUBLISHED 6 AUGUST 2019
- A PRIVACY INFORMATION MANAGEMENT EXTENSION TO ISO/IEC 27001/27002
- REQUIRES ISO 27001 CERTIFICATION
- SETS STANDARDS FOR IMPLEMENTING AND MAINTAINING A PRIVACY INFORMATION MANAGEMENT SYSTEM (PIMS) FOR COMPLIANT PERSONAL DATA MANAGEMENT
- CERTIFICATION OBTAINED 18 NOVEMBER 2019

STEPS TO ISO 27701 CERTIFICATION

Organizations that are ISO 27701 certified and looking to implement the requirements of ISO 27701 should consider taking the following steps:

- Perform a gap assessment of the existing Information Security Management System (ISMS) to the requirements of ISO 27701 and produce an action plan on how to address those gaps
- Conduct a data mapping of the PII collected by the organization to understand the scope of PII collected and how it is used and shared with processors
- Determine the organization's role as a controller and/or processor based on internal or external factors that are relevant to its context, such as applicable privacy legislation, regulations, judicial decisions or contractual requirements (among others)
- Review and update privacy policies to ensure they contain the required information
- Develop policies and procedures applicable to the organization's role
- Begin the planning and implementation of the privacy by design and default principles

PIMS OPERATIONAL OVERVIEW

SCOPE OF PIMS

Personal data processing activities of global Client Data Protection (CDP) accounts across all Operating Groups and risk tiers, (“Client Service Business”), plus the **personal data controllership activities of global Geographical Units** and the supporting global Business Functions, (“Enterprise). See ***PIMS Operational Overview***.

PIMS COMPONENTS AND CONTROLS IN RELATION TO ISO 27701

All controls of the ISO 27701 standard are **applicable.**

PIMS OBJECTIVES

- Establish commitment to **continual improvement**, including through certification and maintenance of an ISO 27701 certification
- **Ensure awareness** of and **compliance with PIMS** related requirements among CDP and Data Privacy personnel who support the PIMS
- Maintain **green scorecard metrics** against privacy controls in Company’s data management tool to validate effective implementation
- Conduct (at minimum) **yearly PIMS Management Reviews** to identify areas of improvement against PIMS performance

RESPONSIBILITIES UNDER THE GENERAL DATA PROTECTION REGULATION

Responsibilities are **set out in individual job descriptions**

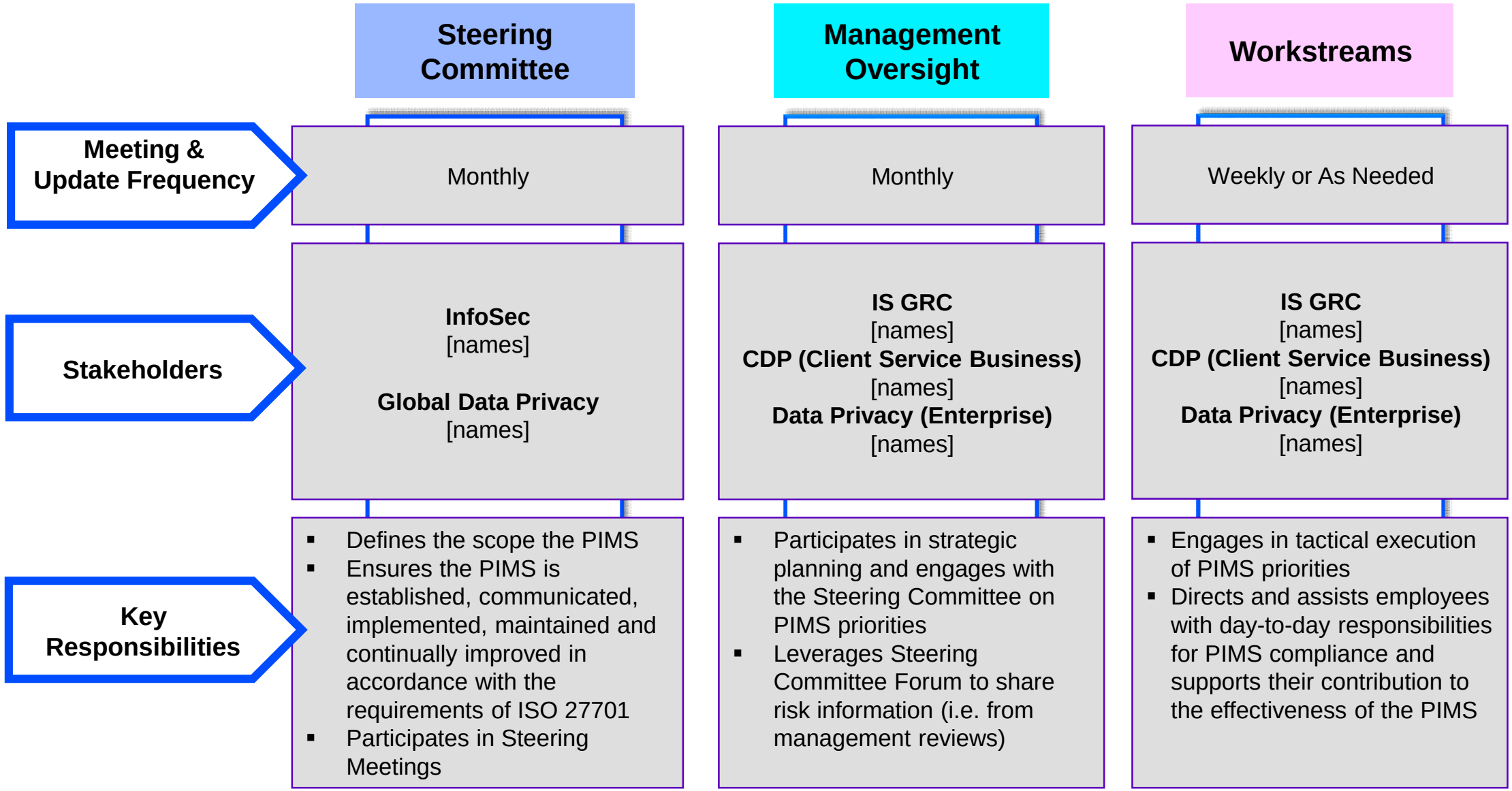
KEY PIMS MANAGEMENT ROLES

- PIMS **Steering Committee**
- PIMS **Executive Sponsor for Enterprise**
- PIMS **Executive Sponsor for Client Service Business**
- PIMS **Operational Oversight**

PIMS MANAGEMENT REVIEW

The structure and process are described in the ***PIMS Management Review Process***

PIMS GOVERNANCE MODEL



ISO 27701

STANDARD AND CERTIFICATION

- REQUIRED CENTRALIZED REVIEW AND GU LEVEL AUDITS IN IBERIA, INDIA, LATAM HSA, ASEAN AND NAM
- AUDITS REQUIRED CLOSE PARTNERSHIP BETWEEN IS, DPISLS AND DATA PRIVACY WITH SUPPORT ACROSS CORPORATE FUNCTIONS
- A COMPREHENSIVE ASSESSMENT OF ACCENTURE DATA PRIVACY PROCESSES AND CONTROLS
- TRACKING SUGGESTIONS BY BSI AUDITORS IDENTIFIED DURING AUDITS AND TO BE ADDRESSED IN SHORT TERM

ASSESSMENT PROCESS

Completed July 26

MANAGEMENT REVIEW

DP and IS GRC
Review of the day-to-day PIMS effectiveness, at least annually or when a change occurs

Completed Aug 29

GAP ANALYSIS WITH BSI

DP and IS GRC
Review of ISO 27701 Standard and checklist of PIMS evidence

Completed Oct 11

STAGE 1 ASSESSMENT

DP and IS GRC
Review of PIMS documentation, recent Management Review report, and previous assessment action plans, if any

Completed Oct - Nov

STAGE 2 ASSESSMENT

DP and GU
Review of implementation of PIMS within selected GUs and Corp Functions that support the GUs

Completed Oct 29

STAGE 2 DATA PRIVACY CENTRAL TOPICS

DP
Review of centrally-managed Data Privacy functions, e.g. global risk assessment, training

ISO 27701

WHAT'S NEXT

- VALIDITY 3 (~2.5) YEARS
- REGULAR MANAGEMENT REVIEWS AND UPDATES TO OUR PIMS
- CONTINUOUS MONITORING MAINTENANCE AUDITS EACH YEAR
- EXPECTATION THAT ISO 27701 WILL AT SOME POINT BE ENDORSED BY EDPB UNDER ART. 42 GDPR
- BE READY FOR RE-CERTIFICATION IN 2022

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

ISO 27701 mapped to CIPL's Accountability Framework

ISO 27701 mapped to CIPL's Accountability Framework

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

PIMS-specific requirements related to ISO 27001
- Context of the organization/ Leadership/ Planning / Support / Operation/ Performance Evaluation Improvement

PIMS-specific requirements related to ISO 27001
- Improvement

PIMS-specific guidance related to ISO 27002
- Human resource security/ Information security incident management

PIMS-specific reference control objectives and controls (PII Controllers)

PIMS-specific requirements related to ISO 27001
- Context of the organization/ Leadership/ Operation/ Performance evaluation

PIMS-specific guidance related to ISO 27002
- Compliance

PII Sharing, Transfer and Disclosure
- Identify basis for PII transfer between jurisdictions/ Countries and international organizations to which PII can be transferred/ Records of transfer of PII/ Records of PII disclosure to third parties

PIMS-specific reference control objectives and controls (PII Processors)
- Customer agreement/ Records related to processing PII

PIMS-specific reference control objectives and controls (PII Controllers)
- Identify and document purpose/ Identify lawful basis/Obtain and record consent/ Privacy impact assessment

PIMS-specific requirements related to ISO 27001
- Support

PIMS-specific requirements related to ISO 27001 :
- Planning /Operation

PIMS-specific guidance related to ISO 27002 :
- Asset Management

PIMS-specific reference control objectives & controls (PII Controllers)
- Privacy Impact Assessment
- Records related to processing PII

PII sharing, transfer and disclosure
- Records of transfer of PII
- Records of PII disclosure to third parties

PIMS-specific reference control objectives and controls (PII Processors)
- Records related to processing PII

PII sharing, transfer and disclosure
- Countries and international organizations to which PII can be transferred
- Records of PII disclosure to third parties

PIMS-specific requirements related to ISO 27001
- Context of the organization / Leadership / Planning / Support/ Operation/ Performance Evaluation/ Improvement

PIMS-specific guidance related to ISO 27002
- Information security policies

Obligations to PII principals
Privacy by design and privacy by default
PII Sharing, transfer, and disclosure
PIMS-specific reference control objectives and controls (PII Processors)

PIMS-specific requirements related to ISO 27001
PIMS-specific guidance related to ISO 27002
PIMS-specific reference control objectives and controls (PII Controllers)
Obligations to PII Principals

Questions?