Keep your customer data safe

Privacy Information Management ISO/IEC 27701

Europrivacy

Presentation

- Welcome
- Your microphone on mute
- During the webinar you can ask your question in the chat, we will try to answer or otherwise we will answer afterwards
- This session will be recorded

David Mudd

- Global Assurance Director Digital Trust

Julien Richard

- Business Development Manager Audit & Certification

Fabrizio Monteleone

- Information Resilience Client Manager

bsi.

Context of this Webinar

- **Compliance:** Global privacy legislations e.g. GDPR, California Consumer Privacy Act, Australian Privacy Act, Japanese Privacy Law (APPI)
- **Reputation risk:** potential brand impact and financial penalties (up to 4% annual revenue or €20M)
- **Trust:** Increased sensitivity and awareness of individual privacy rights
- **Confidence:** Need to demonstrate accountability for managing personally identifiable information
- **Reinforcement:** BSI customer survey revealed common client challenges:
    - managing and securing information
    - preventing a data breach
    - protecting personal information

bsi.

Who are we?

BSI is the business improvement company that enables organizations to turn standards of best practice into habits of excellence.

For over a century BSI has championed what good looks like and driven best practice in organizations around the world.

BSI services worldwide

Knowledge

- Standards development
- Services
- Information solutions

Assurance Services

- Systems certification
- Product certification
- Training
- Customized audit
- BSI Connect (Software)

Regulatory Services

- System- and product certification of medical devices

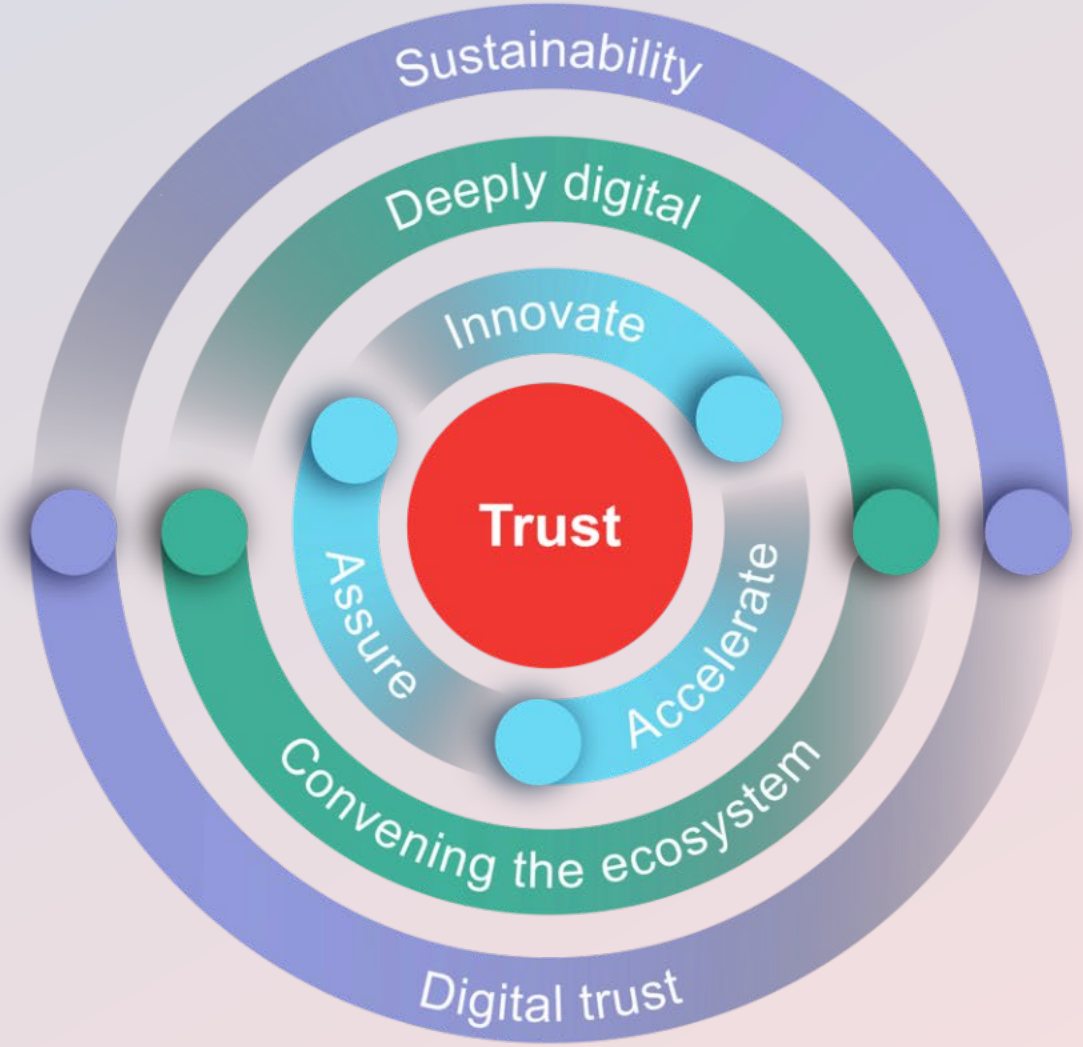
Professional Services

- Supply chain solutions
- Consultancy (environmental, health and safety, security – digital trust and sustainability)

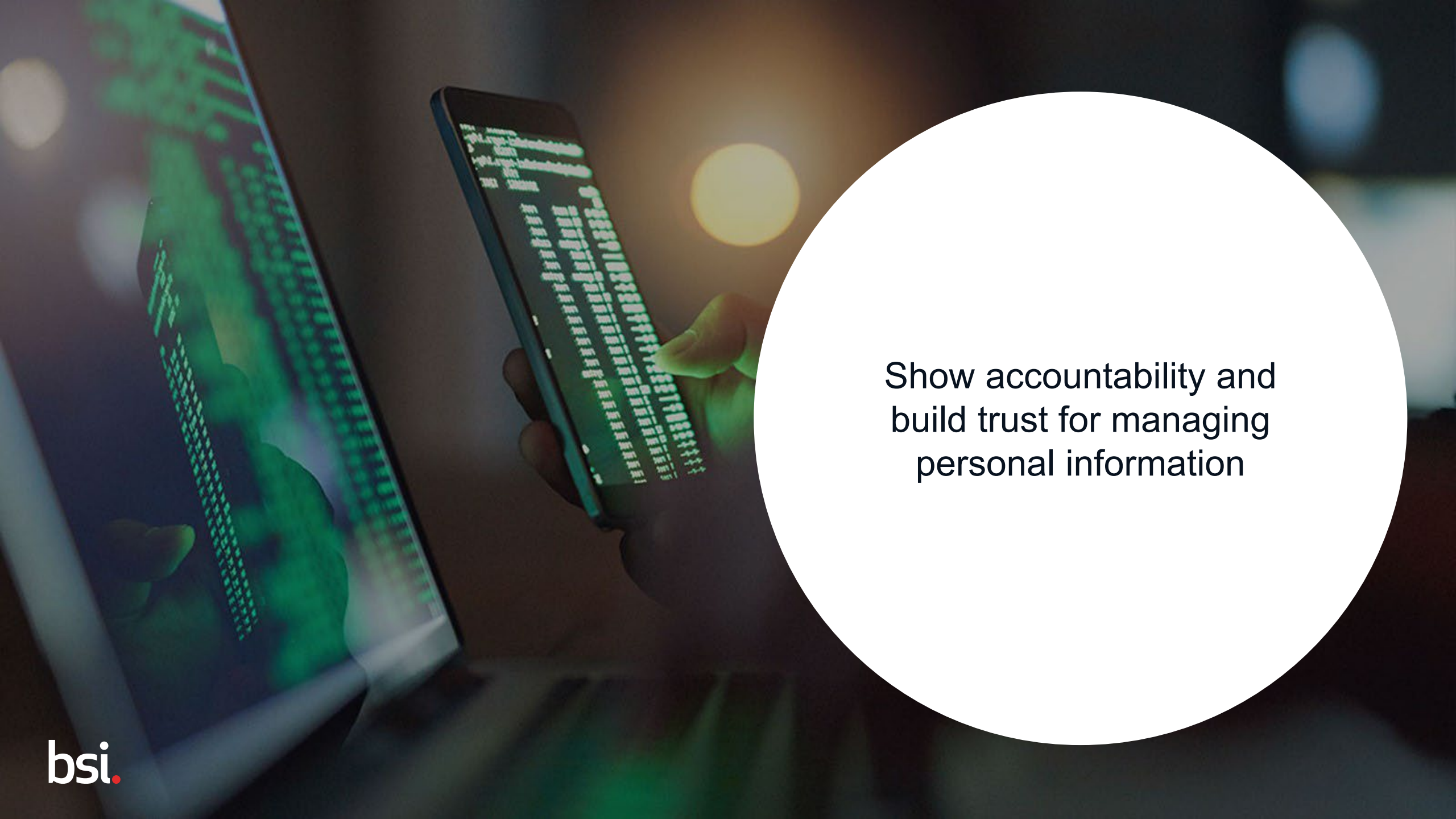
bsi.

As an accredited certification body, BSI Assurance cannot offer certification to clients where they have also received consultancy from another part of the BSI Group for the same management system. Likewise, we do not offer consultancy to clients when they also seek certification to the same management system.

Our vision



bsi.



Show accountability and build trust for managing personal information

Market drivers

132

Global privacy laws and regulation

Up to 4% annual revenue or €20M

Potential fines / penalties

Global Information Security Spending to exceed $124B in 2019
- privacy concerns is driving demand

US$158 Billion

Data protection market 2024
15% CAGR*
(2017-2024)

$2.4 billion

Indication of Fortune 100 spend on managing privacy

bsi.

* Compound Annual Growth Rate

Healthcare specific drivers

Healthcare specPatient records detail some of our most personal details

Globally, specific requirements exist e.g.

- HIPPA US
- HDC France
- My health record (AU)

Mobility and aerospace specific

Privacy is a concern and collected everywhere

For example, passenger travel (e.g. airplanes, uber/lyft/grab) requires sharing of sensitive personal information with the provider but also boarder control, sub-contractors (e.g. the driver, maintenance etc.)

Large fines issued for failing to secure personal records

ISO 27701 and Europrivacy™: Main Differences

ISO 27701:2019

Standard specifying requirements to certification of a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization.

Accreditation = ISO 17021 related to Management Systems.

Cannot be used to claim conformity to GDPR – not fulfilling requirements of GDPR Art. 42 and 43,1, b).

Europrivacy™

Scheme which provides all the requirements to enable certification of data processing compliance to the:

GDPR; Complimentary National data protection regulations; Domain specific data protection regulations

Accreditation = predominantly ISO/IEC 17065 – Assessing data processing operations related to product, processes and services (PPS) and ISO/IEC 17021-1 – Assessing the Data Protection Management Systems (DPMS)

bsi.

ISO 27701:2019

POLL 1

If you have a formal Privacy Information Management System in place, how does it relate to ISO 27701?

- We don’t have Privacy Information Management System in place.
- Use ISO 27701 as a framework but we don’t want to certify
- Don’t use ISO 27701 as a framework but we plan to use
- Don't use ISO 27701 as a framework. No plans to move towards.
- Use ISO 27701 as a framework and we're planning to certify

bsi.

ISO IEC 27701: WHAT IS IT FOR

Why ISO 27701

- **ISO/IEC 27701,** was published in August 2019 to take on data privacy and PII treatment
- **Title of the standard** is "Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management"
- It’s an **ISO/IEC 27001 add-on** meaning that can be implemented only if an ISO/IEC 27001 management system is in place.

bsi.

Who should use ISO/IEC 27701?

- All types and sizes of organizations
- Public and private companies, government entities and not-for-profit organizations
- Organizations responsible for PII processing within an information security management system (ISMS), specifically:
  - PII controllers (including those who are joint PII controllers)
  - PII processors

bsi.

ISO 27701 requirements

Principal chapters to focus on:

5) PIMS specific requirements related to ISO/IEC 27001

6) PIMS specific guidance related to ISO/IEC 27002

7) Additional guidance for PII Controllers

8) Additional guidance for PII Processors

ISO 27701 Annexes

- The ISO/IEC 27701 includes several Annexes:
- A and B are for controllers and processors respectively,
- Annexes C – F provide additional knowledge that can support with setting up and operating an effective PIMS.

Benefits ISO/IEC 27701 provides

- Builds trust in managing personal information
- Provides transparency between stakeholders
- Facilitates effective business agreements
- Clarifies roles and responsibilities
- Supports compliance with global privacy regulations
  (e.g. EU GDPR, Japanese Act on Protection of Personal Information)
- Reduces complexity by integrating with the leading information security standard ISO/IEC 27001

bsi.

ISO/IEC 27701 certification with BSI includes…

- Gap assessment (optional)
  See how close you are to meeting the requirements before your formal assessment visit

- Formal assessment
  This is a two-stage process to make sure your PIMS is working effectively as required for ISO/IEC 27701 certification. The length varies depending on quantity and type of PII your organization is accountable for

- Continual Surveillance audits
  We will continue to visit you each year to ensure your PIMS adds maximum value

bsi.

Why BSI for ISO/IEC 27701?

- BSI has been at the forefront of **information security standards** since 1995
- We produced the **world's first** standard –
  BS 7799, now ISO/IEC 27001 - the **world's most popular** information security standard
- And we haven't stopped there, addressing the **new emerging issues** such as privacy, cyber and cloud security
- We have the technical know-how and networks to drive the privacy agenda for both organization and society

bsi.

EUROPRIVACY™

WHAT IS IT FOR?

POLL 2

Why do you think the Europrivacy™ certification can be relevant for you organization?

- It helps us to identifying, reducing the risks with analysis
- It demonstrates that our organization is complying with GDPR
- Competitive advantages, reputation improvement, confidence
- It’s important but not our priority now

BSI & EUROPRIVACY

BSI is Qualified as Partner Certification Body of Europrivacy, by the European Centre for Certification and Privacy (ECCP).

BSI can certify client's conformity of their data processing activities with Europrivacy and the European General Data Protection Regulation (GDPR)

bsi.

EUROPRIVACY ECOSYSTEM

The certification scheme: audit criteria overview

- Certification to the Europrivacy Scheme can only be applied to:
  - processing activity contained within a specific product, process or service
  - offered by a Controller or Processor

The certification scheme: what can be certified

- ToE = Target of Evaluation, e.g. processing activity contained within a specific product, process or service
- Offered by a Controller or Processor

bsi.

Some examples *:

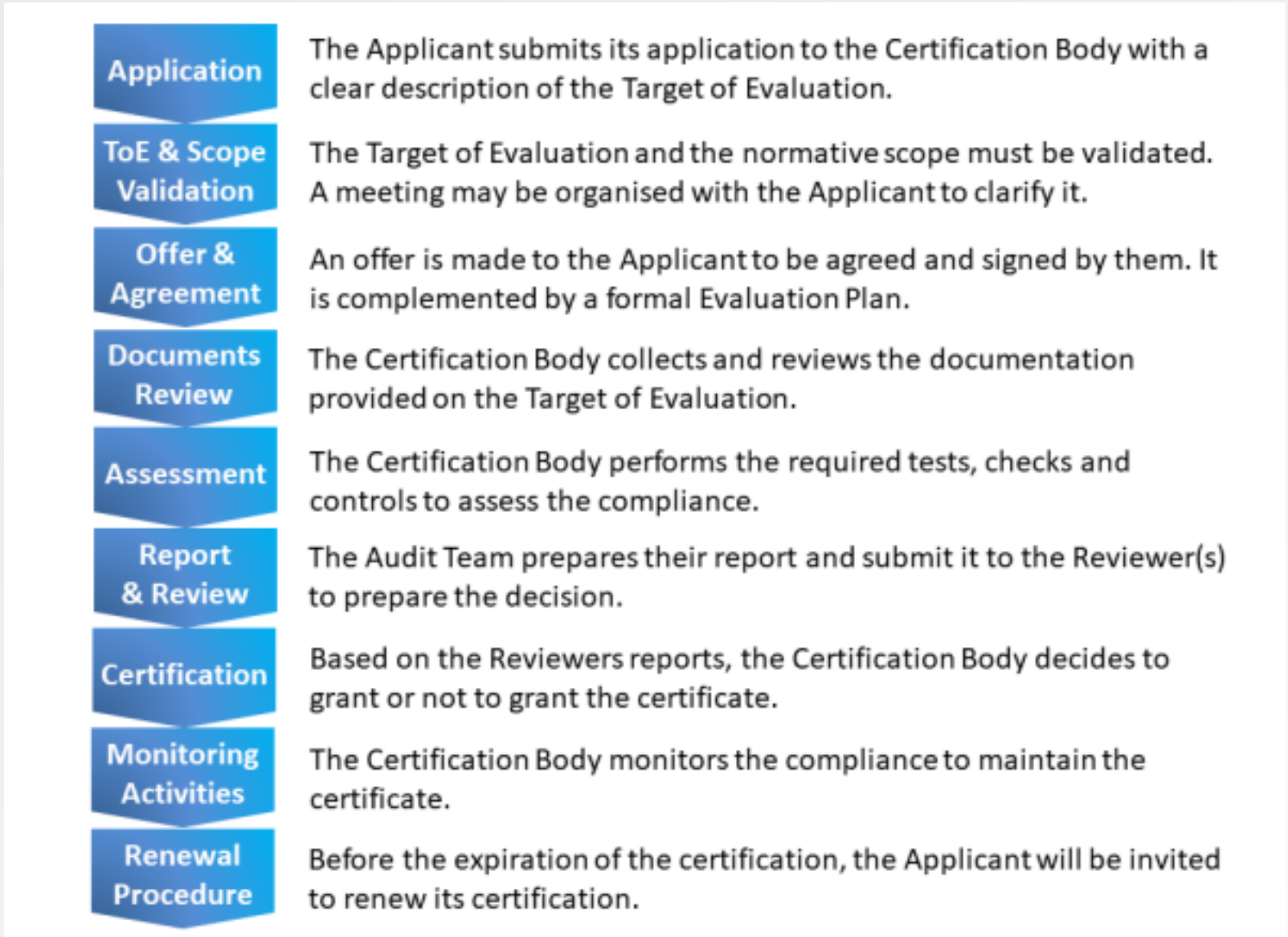
*edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en

1): A “Privacy Seal” offering a general scope only requiring “a specification of the processing subject to certification” would not provide clear enough guidance on how to set and describe a ToE.

2) A ToE describing in sufficient detail the processing operation of a web based service such as including the registration of users, the provision of service, invoicing, logging of IP-addresses, interfaces to users and to third parties and excluding server hosting (yet including processing and TOM agreements) can be accepted.

bsi.

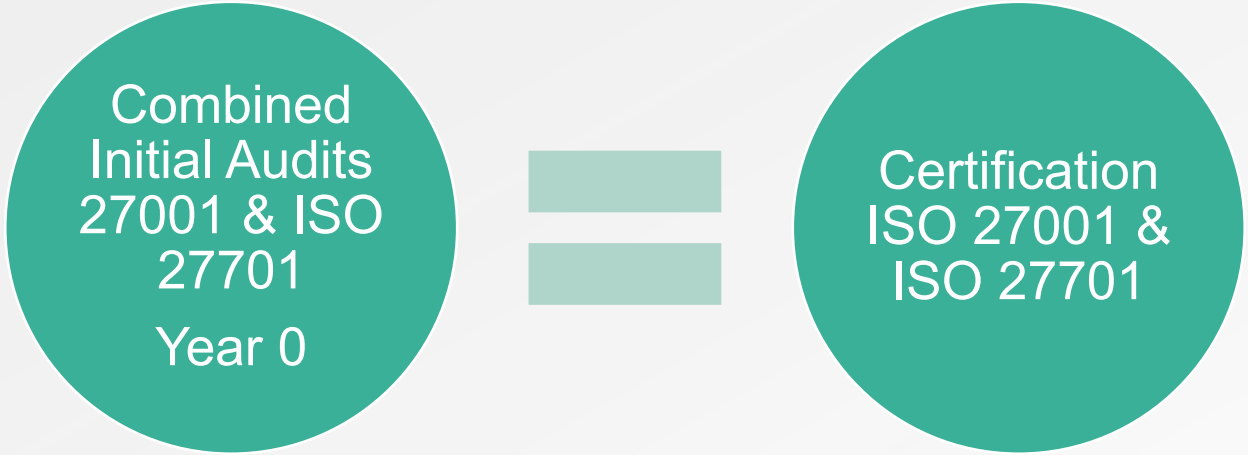
Certification Process



ISO 27701
Certification Process

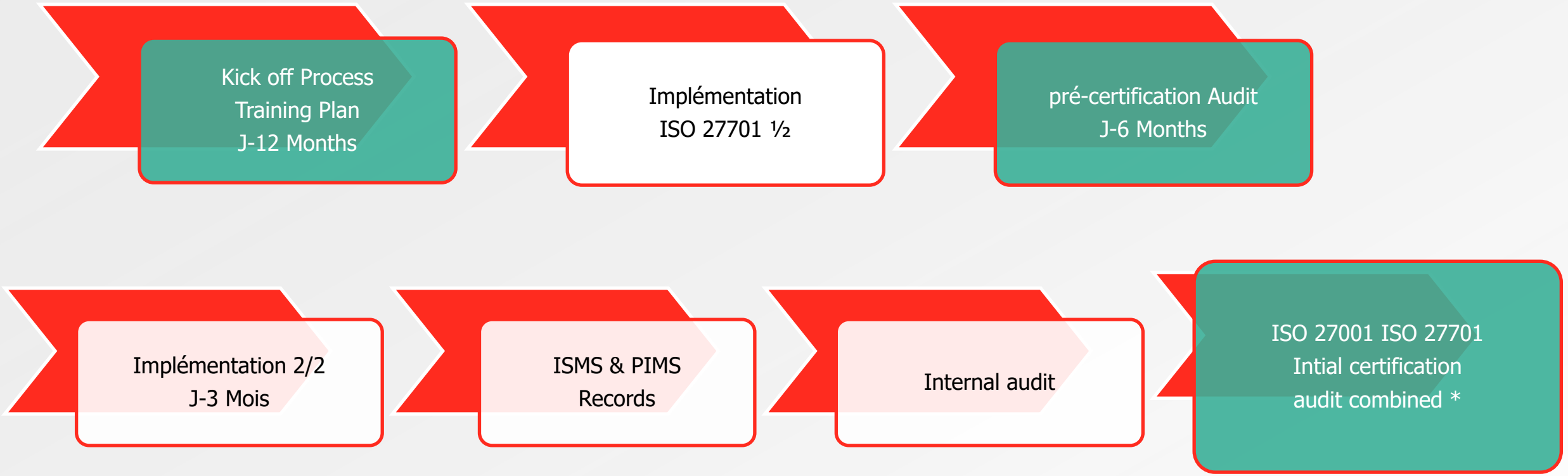
Key Information

Two Certifications Process



bsi.

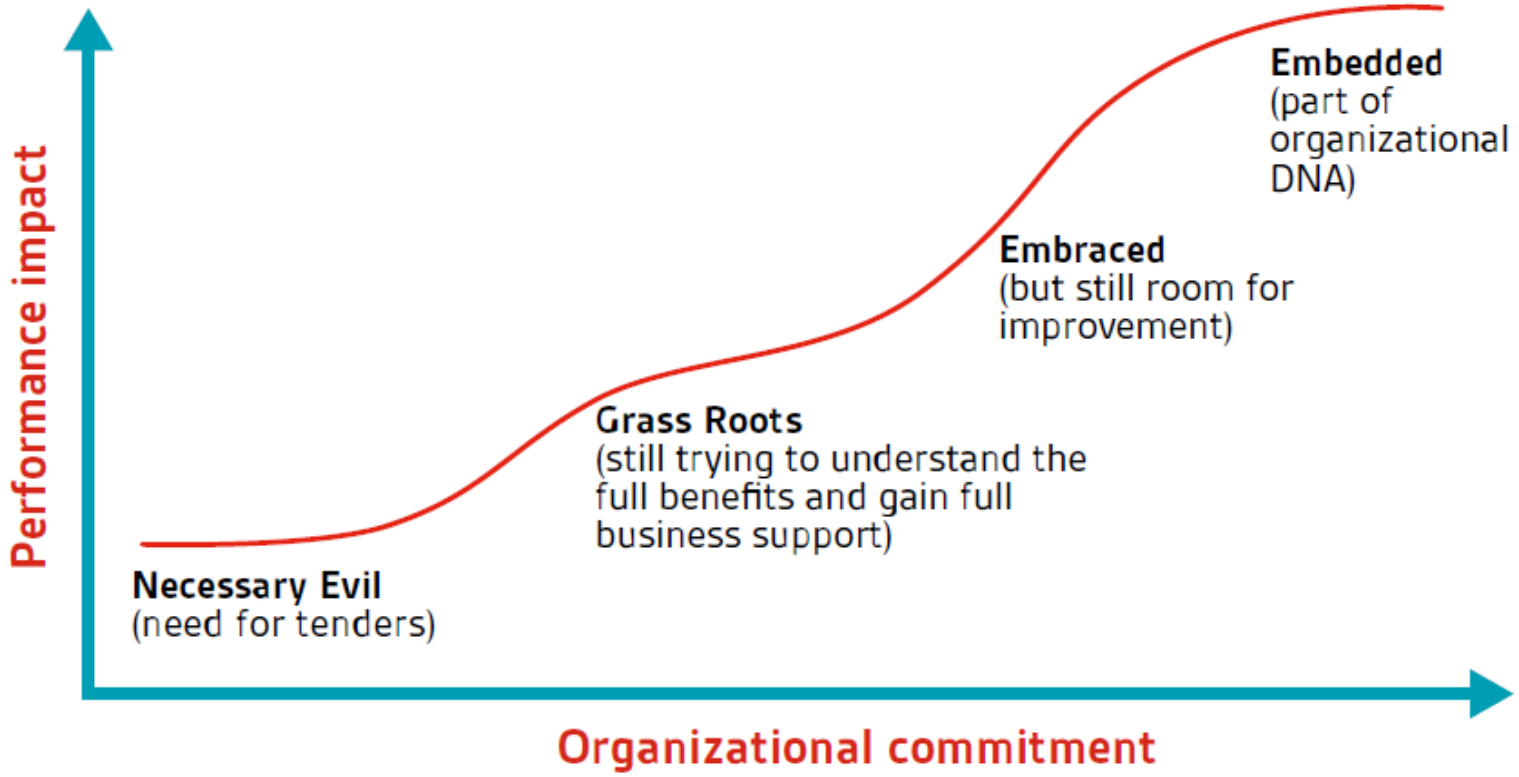
Key Steps ISO 27701 Certification Plan



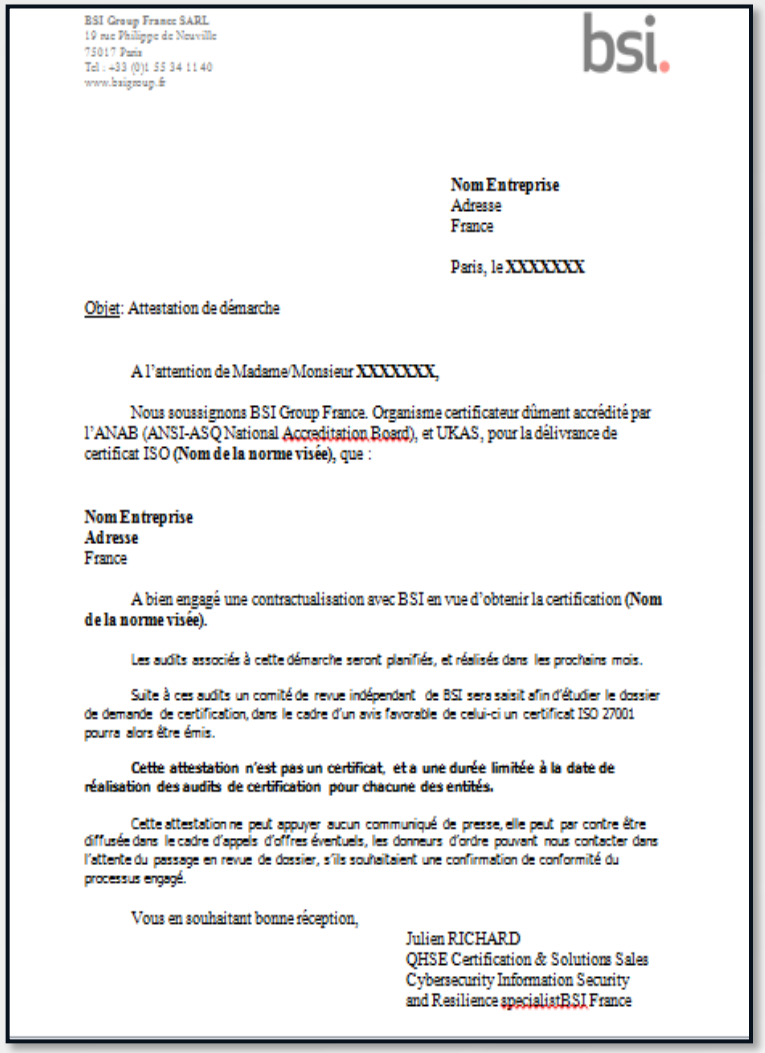
* In the case where Certification Body si the same for the 2 standards

bsi.

Our Mission, Help your organization to increase performance, and develop your management system maturity and resilience



Benefits **ISO 27701 BSI Services Engagement Letter**



BSI Group France SARL
19 rue Philippe de Neuville
75017 Paris
Tel : +33 (0)1 55 34 11 40
www.bsigroup.fr

Nom Entreprise
Adresse
France

Paris, le XXXXXXX

Objet: Attestation de démarche

A l'attention de Madame/Monsieur XXXXXXX,

Nous soussignons BSI Group France. Organisme certificateur dûment accrédité par l'ANAB (ANSI-ASQ National Accreditation Board), et UKAS, pour la délivrance de certificat ISO **(Nom de la norme visée)**, que :

Nom Entreprise
Adresse
France

A bien engagé une contractualisation avec BSI en vue d'obtenir la certification **(Nom de la norme visée)**.

Les audits associés à cette démarche seront planifiés, et réalisés dans les prochains mois.

Suite à ces audits un comité de revue indépendant de BSI sera saisit afin d'étudier le dossier de demande de certification, dans le cadre d'un avis favorable de celui-ci un certificat ISO 27001 pourra alors être émis.

Cette attestation n'est pas un certificat, et a une durée limitée à la date de réalisation des audits de certification pour chacune des entités.

Cette attestation ne peut appuyer aucun communiqué de presse, elle peut par contre être diffusée dans le cadre d'appels d'offres éventuels, les donneurs d'ordre pouvant nous contacter dans l'attente du passage en revue de dossier, s'ils souhaitaient une confirmation de conformité du processus engagé.

Vous en souhaitant bonne réception,

Julien RICHARD
QHSE Certification & Solutions Sales
Cybersecurity Information Security
and Resilience specialistBSI France

After Validation of a ISO 27701 Contract, BSI Will edit an engagement letter which will confirm than your organization is well engaged in ISO 27001 / ISO 27701 implementation plan, and than certification audit will be realized in the next comings months

This letter could be send to your prospects, clients, partners, and give opportunity to implement in better condition, with a timeline more adapted and less market presssion

ISO/IEC 27701 Training Plan

- **Our In house training** Plan help all your team involve in PII to increase their knowledge, understanding and capacity to implement actions Plan to get and maintain certification
- **ISO/IEC 27701 - Introduction**
  Understand what is a PIMS and standard requirement : 1 Jour
- ISO/IEC 27701 - Implementing
  Get skills to implement an ISO 27001 PIMS : 2 Days
- ISO/IEC 27701 – Internal audit
  Get skills to be able to realize ISO 27701 Internal audit (for current ISO 27001 internal auditor) : 1 Jour

Why BSI Mark of Trust for your ISO/IEC 27701 Certification Process?

- We produced the world's first standard – BS 7799, now ISO/IEC 27001 - the world's most popular information security standard
- BSI Assurance Mark is the most important certification Mark in Information security and Privacy globally
- Our rigorous assessments, will help you to increase your organization performance, and your capacity of adaptation to market and compliance requirements
- Worldwide Label recognized in more than 150 countries will support you in your market development

bsi.

POLL 3

If you should define your company engagement in Data Privacy / Digital Trust, how do you'd define it?

- We are approaching and this is still new for our business
- We have recently established a programme of development.
- We have a well-established programme
- We have a mature programme in place

bsi.

Time for questions

Start with questions

And Now, what next steps we propose to you

- Send to You Presentation
- If you want Answer directly to your questions during individual meeting

- And If you want
  - Realize a first evaluation of compliance data privacy scope,
  - Present to you estimation of Certification Budget

bsi.

Thank you! Keep in contact?

- **Julien Richard**
  Julien.Richard@bsigroup.com

- **Fabrizio Monteleone**
  Fabrizio.Monteleone@bsigroup.com

Send PP slides?