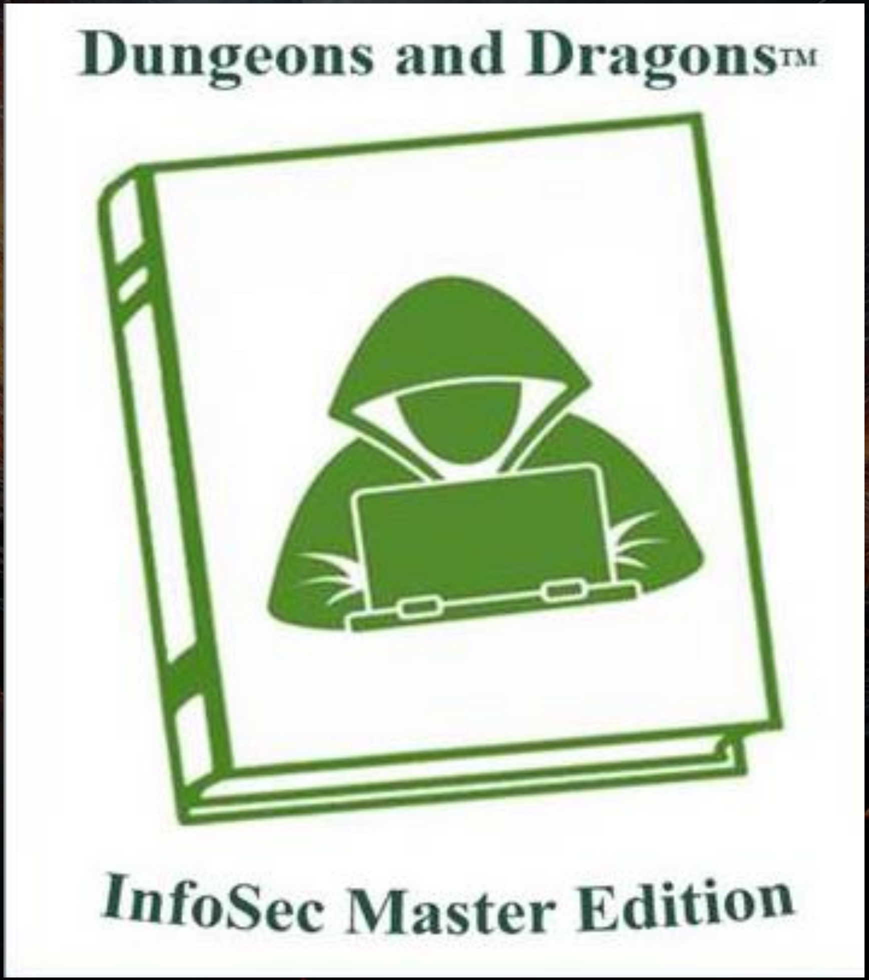
Welcome To The 10th Annual Hacking Conference



The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

Welcome To The 10th Annual Hacking Conference

Remember to check-in to this session on the app!

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

schellman

Optimize Your Information Security and Data Privacy Program with the ISO 27000 Family of Standards

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

Presenters

Danny Manimbo

Principal / ISO Practice Co-Director

Based in Denver, CO

danny.manimbo@schellman.com

schellman Quality, above all.

Chris Lippert

Senior Manager / Privacy Practice Lead

Based in Atlanta, GA

chris.lippert@schellman.com

schellman Quality, above all.

Schellman Suite of Services Overview

SOC Examinations

SOC 1 / SSAE 18
SOC 2
SOC 3
SOC for Supply Chain
SOC for Cybersecurity
C5 Attestation
CSA STAR Programs

ISO Certification

ISO 9001
ISO 20000-1
ISO 22301
ISO 27001
ISO 27018
ISO 27701

Federal Assessments

FedRAMP
CMMC / NIST SP 800-171
FISMA / NIST 800-53
CJIS
ITAR

Payment Card Assessments

PCI DSS
PCI SSF
PCI P2PE
PCI PIN
PCI 3DS
PCI ASV

Cybersecurity Assessments

Crypto & Digital Trust
NY DFS Assessment
NIST CSF Assessment
C5 Assessment
Software Security Assessment (S3A)

Healthcare Assessments

HITRUST CSF
HIPAA
HIPAA Express
EPCS-DEA Audits
Health Data Host (HDS)

Penetration Test Testing

Application
Network
Mobile
Social Engineering
Cloud
Secure Code Review
Hardware & IoT
Advanced Services

Privacy Program Assessments

APEC Certification
GDPR
International Privacy
US State Privacy
Microsoft SSPA / DPR
FERPA
EU Cloud Code of Conduct
CCPA

Financial Services Assessments

SWIFT CSP
FFIEC
GLBA
Cybersecurity

Automotive Assessments

TISAX Audit Provider

ESG & Sustainability

ESG Assessments
ESG Assurance

Training Services

On-Demand Training
Instructor-Led Bootcamps
Certification Courses

ISACA Chicago Chapter

Agenda

1. ISO 27000 Family of Standards Overview
2. ISO 27001 Certification Alignment with Sector-Specific ISO 27000 Standards
3. Data Privacy Program Enhancement via Adoption of ISO 27018 and/or ISO 27701
4. EU Cloud Code of Conduct, Europrivacy GDPR Certification/Seal, and CBPR/PRP
5. Q&A

1

ISO 27000 Family of Standards Overview

ISO 27000 Family of Standards Overview

- ISO 27001 most well-known
- Additional best practices in data protection and cyber resilience covered by other ISO 27000 standards
- Standards related to security & privacy we'll cover today include:
  - ISO 27001 (ISMS) – the foundational element
  - ISO 27017 (cloud services security)
  - ISO 27018 (protection of PII in public clouds for PII processors)
  - ISO 27701 (PIMS) – and complementary GDPR certification frameworks such as Europrivacy Seal and the overlap with the EU Cloud Code of Conduct

ISACA Chicago Chapter

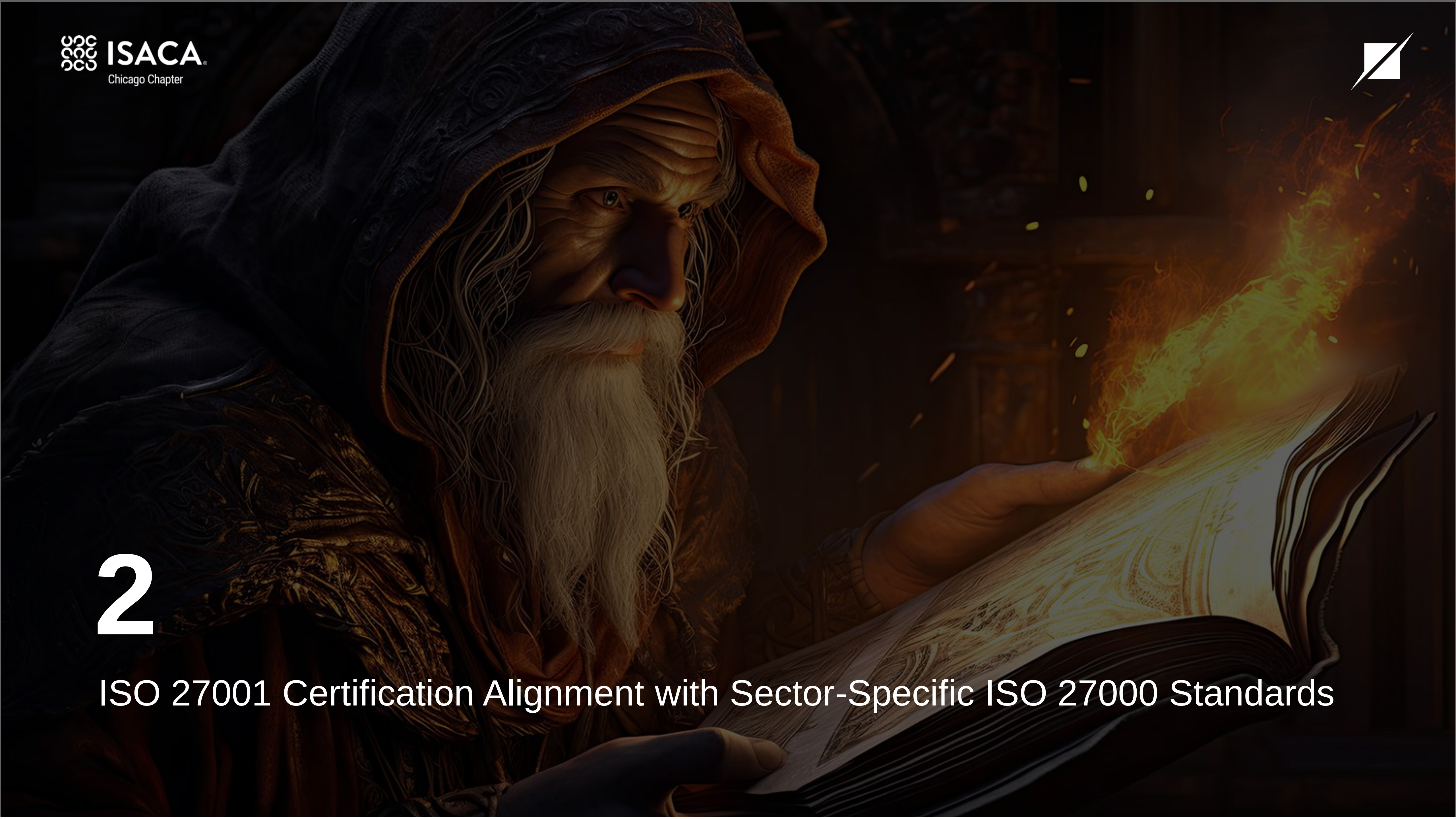
ISO 27000 Family of Standards Overview

Standard / Metric	ISO 27001	ISO 27017	ISO 27018	ISO 27701
Purpose	Requirements for establishing, implementing, maintaining and continually improving an **information security management system (ISMS)**	Cloud-specific implementation guidance based on ISO 27002 and additional controls to address **cloud-specific information security threats and risk considerations**	Establish commonly accepted control objectives, controls, and guidelines for implementing measures to **protect PII** in line with the privacy principles in ISO 29100 for the **public cloud computing environment** and specifies guidelines based on ISO 27002, taking into consideration the regulatory requirements for PII protection	Requirements and guidance for establishing, implementing, maintaining and continually improving a **privacy information management system (PIMS)** in the form of an extension to ISO 27001 and ISO 27002
Main Topic Areas (Ex:)	ISMS preserving the CIA of information by applying a risk-based approach and adoption of controls (Annex A)	Shared R&R Data segregation VM hardening Service monitoring	Consent and choice Purpose legitimacy and specification Collection limitation	Conditions for collection & processing Obligations to PII principals Privacy by design & default

ISACA Chicago Chapter

ISO 27000 Family of Standards Overview

Standard / Metric	ISO 27001	ISO 27017	ISO 27018	ISO 27701
Intended User(s)	Any organization	Cloud service providers (CSP) and cloud service customers (CSC)	CSPs who process PII	Any organization which are PII controllers and/or PII processors processing PII within an ISMS
Management System Framework	Yes – ISMS	No – Control Set Only	No – Control Set Only	Yes – PIMS
Control Count	114 (:2013) 93 (:2022)	7	25	31 (Clause 7 / Annex A) 18 (Clause 8 / Annex B)
Current Version	ISO 27001:2022*	ISO 27017:2015	ISO 27018:2019	ISO 27701:2019
Aligned with ISO 27001/2:2022	N/A	No	No	No
Updates in Progress	**Transition period in progress*	Yes – Committee Draft (CD)	No	Yes – Draft International Standard (DIS)



2

ISO 27001 Certification Alignment with Sector-Specific ISO 27000 Standards

ISO 27001 Certification Alignment – General

- ISMS considerations of adding sector-specific standards (modifications to):
  - Scope statement
  - Objectives
  - Risk assessment / risk treatment
  - Statement of applicability
  - Metrics / KPIs
  - Internal audit
  - Management review (input / outputs)

ISO 27001 Certification Alignment – ISO 27017

ISO 27017 Considerations – Cloud Services Security	
Target / Objective ("The Why")	Designed to be utilized for CSPs as well as CSCs to help ensure that, for either role, proper controls and implementation guidance have been designed and applied related to the cloud service
Level of Effort to Align to Existing ISMS	Moderate
Considerations	- Determination of role (CSP vs. CSC) - Entities acting as CSP, or providing cloud-based services, to Canadian (SPIN) or Italian (Cloud Italy Strategy) governments

ISO 27001 Certification Alignment – ISO 27018

ISO 27018 Considerations – Protection of PII in Public Cloud	
Target / Objective (“The Why”)	- Helps public cloud service providers (PCSP) comply with applicable obligations (contracted or not) when acting as PII processor - Enable public cloud PII processor to be transparent to enable CSCs to select well-governed cloud-based PII processing services - Assist CSC and public cloud PII processor in entering into a contractual agreement - Provide CSCs a mechanism for exercising audit and compliance rights and responsibilities
Level of Effort to Align to Existing ISMS	Moderate
Considerations	- Entities acting as CSP, or providing cloud-based services, to Italian (Cloud Italy Strategy) government - Weighing options of ISO 27018 (control set) vs. ISO 27701 (management system) - Some guidelines applicable to PII controllers, but standard is not intended to cover additional obligations of PII controllers

ISO 27001 Certification Alignment – ISO 27701

ISO 27701 Considerations – PIMS	
Target / Objective ("The Why")	Can be used by PII controllers (including those that are joint PII controllers) and PII processors (including those using subcontracted PII processors and those processing PII as subcontractors to PII processors) to demonstrate privacy protection practices in the processing of PII
Level of Effort to Align to Existing ISMS	High
Considerations	- Applicable to both PII controllers and / or processors - More robust than ISO 27018 (control set only) in that it's both a management system and supporting controls framework

Polling Question 1

Which of the following statements is correct as it relates to the ISO 27001, ISO 27701, ISO 27017, and ISO 27018 standards?

a) All standards are management system frameworks.

b) Only ISO 27001 is a management system framework, the remainder are control sets only.

c) Only ISO 27001 and ISO 27701 are management system frameworks, ISO 27017 and ISO 27018 are control sets only.

d) All standards are management system frameworks.

3

Data Privacy Program Enhancement via Adoption of ISO 27018 and/or ISO 27701

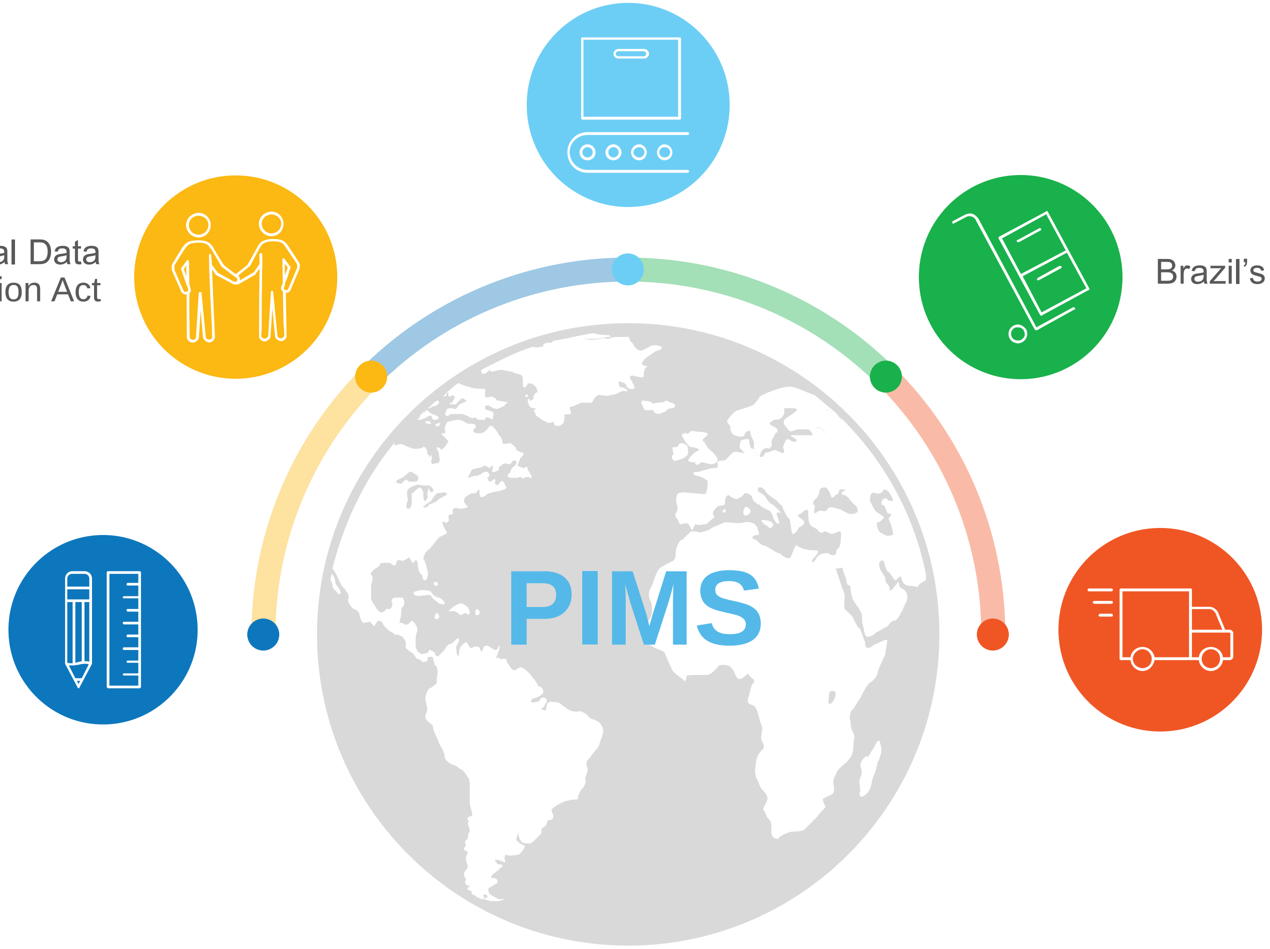
ISO 27018 Overview

- 27018 supplements the ISO/IEC 27001:2013 control set within Annex A with 25 extended controls unique to cloud service providers.
- These unique controls are associated with the 11 privacy principles within ISO 29100 and address topics such as:
    - Consent and choice
    - Purpose legitimacy and specification
    - Data minimization
    - Use, retention and disclosure
    - Openness, transparency and notice
    - Accountability
    - Information security
    - Privacy compliance

ISO 27701 Overview

- ISO 27701 ISO 27701 is valuable to organizations that have an existing ISO 27001 certification or are considering an ISO 27001 certification and want to include their privacy program into their ISMS. An accredited ISO 27001 certification that includes ISO 27701 demonstrates an organization’s security and privacy practices through a validated third-party assessment.
- ISO 27701 applies to any organization operating in any part of the world
- ISO 27701 is not a standalone certification – it is an extension of the ISO 27001 certification
- It requires development and maintenance of a PIMS in addition to the current ISMS or as a separate system. It also includes additional controls for both controllers and processors.

The Scope and Criteria of ISO 27701



Australia’s Privacy Act / Principles

The EU’s General Data Protection Act

Brazil’s LGPD

California’s Consumer Privacy Act

PIMS

Canada’s PIPEDA

Clause 5

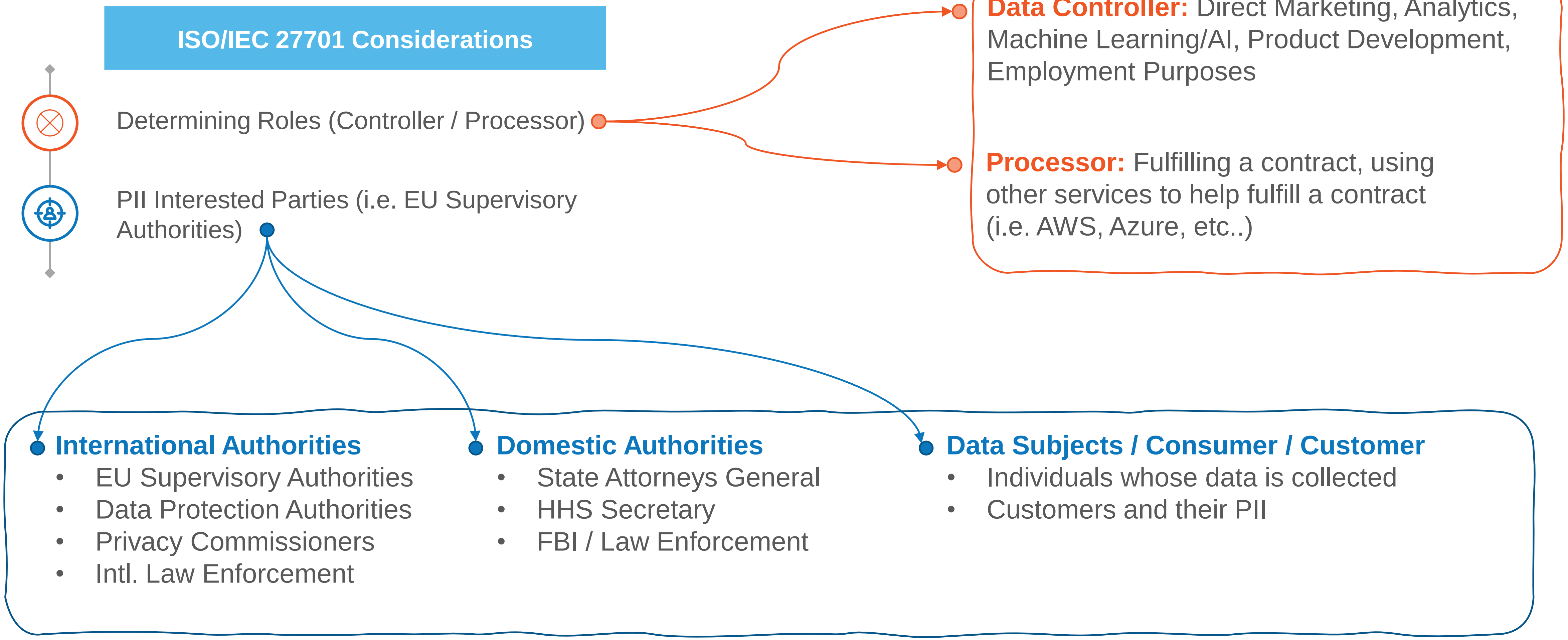
	ISO/IEC 27001:2013 Requirement	+	ISO/IEC 27701 Considerations
5.2.1	Understanding the Organization and its context		Have PII processing roles (Controller / Processor) been established?
5.2.2	Understanding the needs and expectations of interested parties		Are PII Interested Parties (i.e. PII Principals, or individual consumers) documented?
5.2.3	Determining the scope of the information security management system		Does the ISMS include processing of PII in the scope statement?
5.2.4	Information security management system		Has PIMS been integrated into the ISMS reviews?
5.4.1.2	Information security risk assessment		Do risk assessments consider PII?
5.4.1.3	Information security risk treatment		Has ISO 27701 Annex A/B been considered in risk assessment / treatment plan?

=

PIMS Program

Clause 5

As an example…



ISO/IEC 27701 Considerations

Determining Roles (Controller / Processor)

PII Interested Parties (i.e. EU Supervisory Authorities)

Data Controller: Direct Marketing, Analytics, Machine Learning/AI, Product Development, Employment Purposes

Processor: Fulfilling a contract, using other services to help fulfill a contract (i.e. AWS, Azure, etc..)

International Authorities

- EU Supervisory Authorities
- Data Protection Authorities
- Privacy Commissioners
- Intl. Law Enforcement

Domestic Authorities

- State Attorneys General
- HHS Secretary
- FBI / Law Enforcement

Data Subjects / Consumer / Customer

- Individuals whose data is collected
- Customers and their PII

Clause 6

- Update policies
- Designate point of contact
- Update training
- Labeling PII
- Encryption of PII in storage
- Secure disposal and transfer of PII
- User registration and de-registration
- Clear desk
- Backups
- Event Logging
- Protection of logs
- Confidentiality agreements
- Encryption of data in transit
- Secure development policies
- Privacy by design
- Protection of test data
- Supplier Agreements
- Data breach identification, recording and notifications
- Identify Legal Sanctions
- Etc

Clause 7 - Controller Specific

- Control Objectives
  - Conditions for Collection and Processing
  - Obligations to PII Principals
  - Privacy by Design and Default
  - PII Sharing, Transfer and Disclosure
- Controls - 31

GET ALL THE INFORMATION YOU CAN, WE'LL THINK OF A USE FOR IT LATER.

Clause 8 - Processor Specific

- Control Objectives
  - Conditions for Collection and Processing
  - Obligations to PII Principals
  - Privacy by Design and Default
  - PII Sharing, Transfer and Disclosure
- Controls - 18

cartoonstock.com

ISACA Chicago Chapter

Polling Question 2

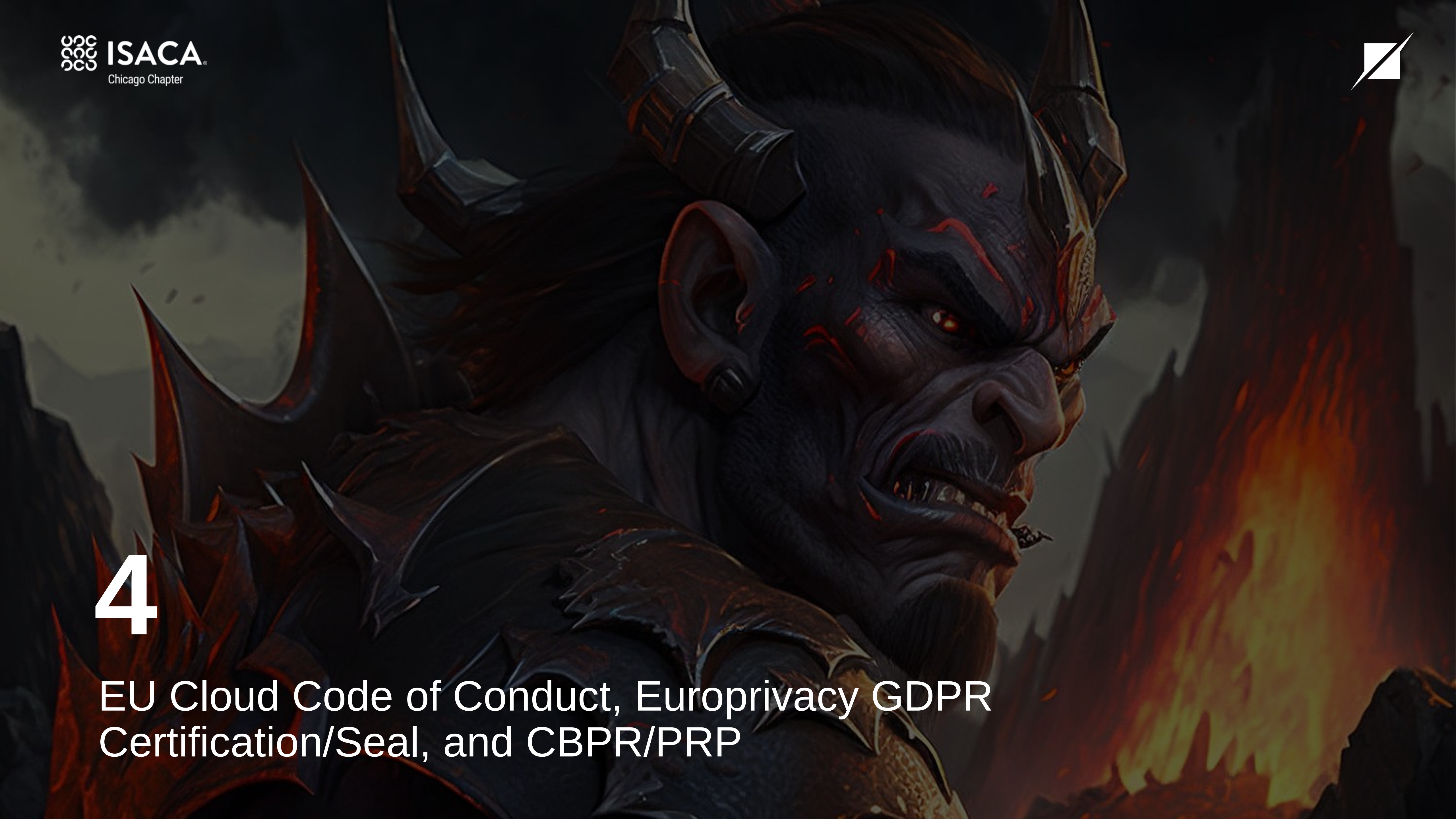
ISO/IEC 27701:2019 is currently being updated to reflect the changes of ISO/IEC 27001:2022. Are organizations allowed to certify against ISO/IEC 27001:2022 and ISO/IEC 27701:2019 or do they need to wait for an updated ISO/IEC 27701 standard?

a) Yes, with no action needed.

b) Yes, with updates to the SOA to speak to new control mappings.

c) Yes, as the two standards don’t rely on each other.

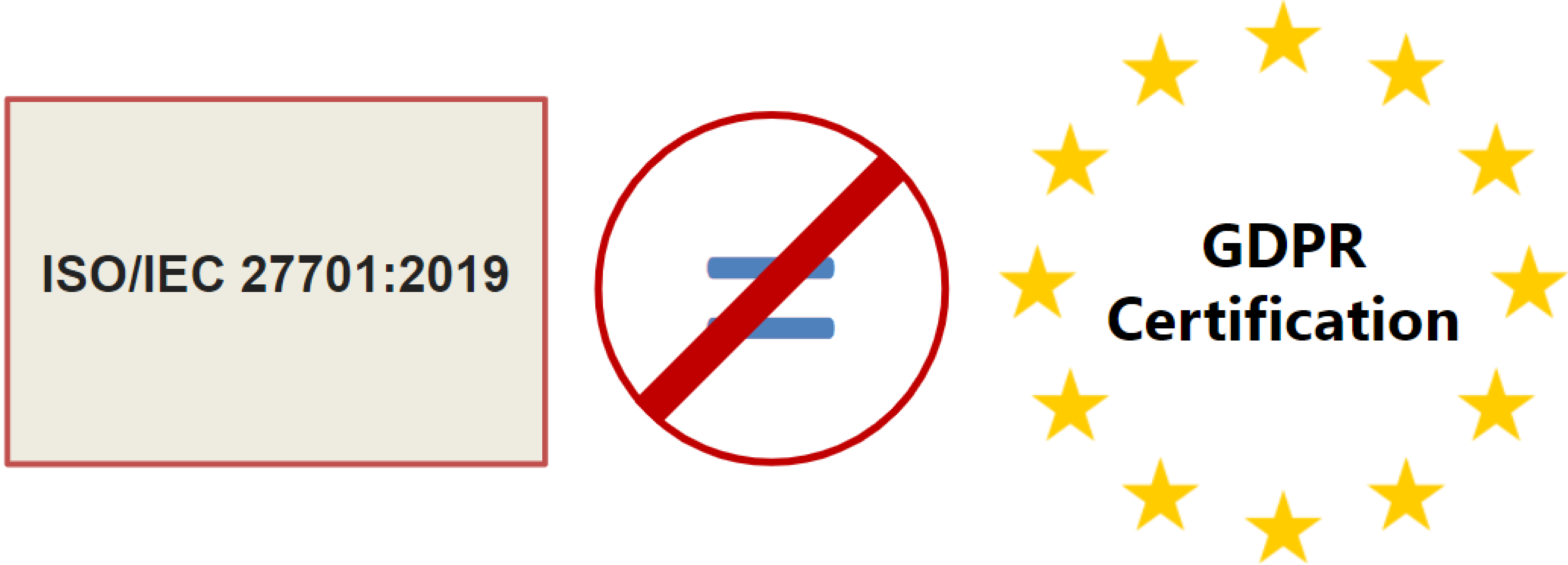
d) No, they have to wait for the new ISO 27701 standard.



4

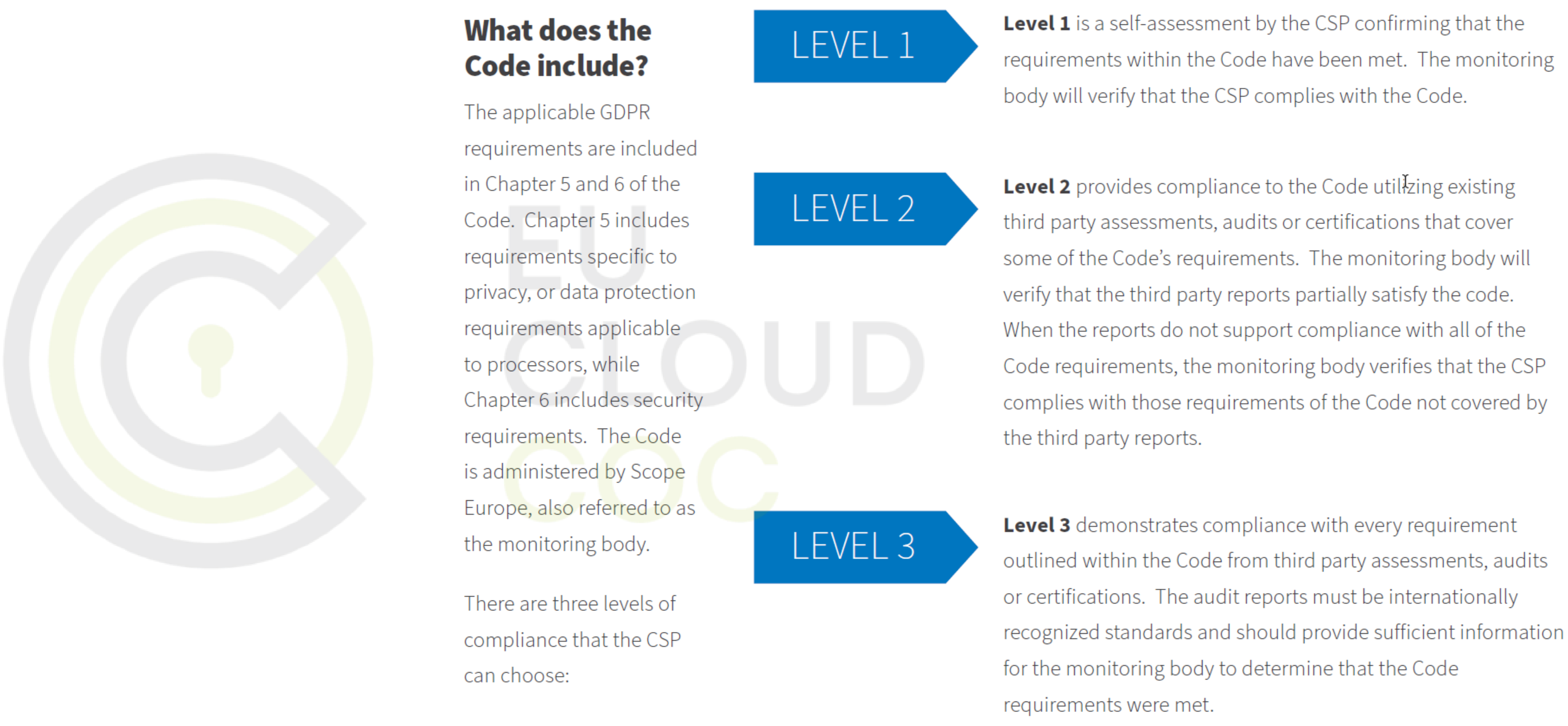
EU Cloud Code of Conduct, Europrivacy GDPR Certification/Seal, and CBPR/PRP

ISO 27701 and GDPR



ISO/IEC 27701:2019 ≠ GDPR Certification

EU Cloud Code of Conduct



What does the Code include?

The applicable GDPR requirements are included in Chapter 5 and 6 of the Code. Chapter 5 includes requirements specific to privacy, or data protection requirements applicable to processors, while Chapter 6 includes security requirements. The Code is administered by Scope Europe, also referred to as the monitoring body.

There are three levels of compliance that the CSP can choose:

LEVEL 1

Level 1 is a self-assessment by the CSP confirming that the requirements within the Code have been met. The monitoring body will verify that the CSP complies with the Code.

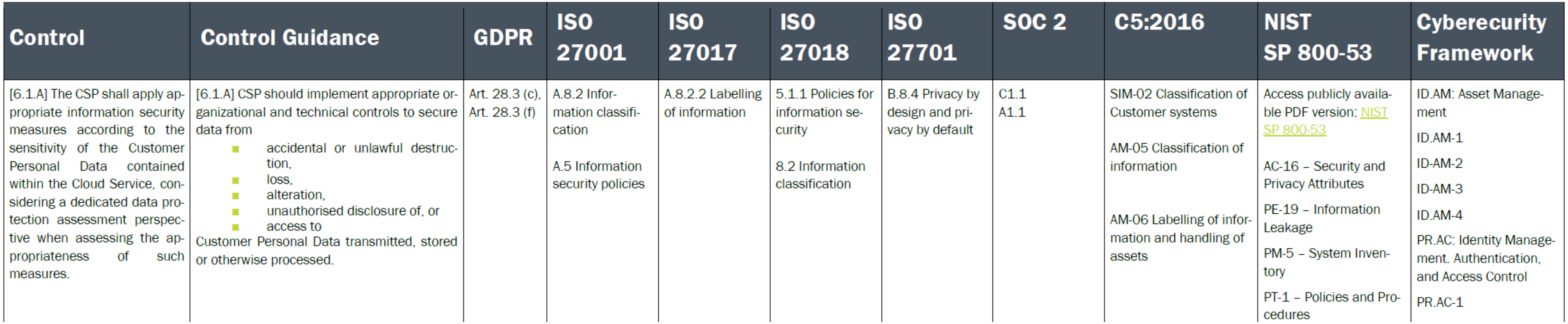
LEVEL 2

Level 2 provides compliance to the Code utilizing existing third party assessments, audits or certifications that cover some of the Code’s requirements. The monitoring body will verify that the third party reports partially satisfy the code. When the reports do not support compliance with all of the Code requirements, the monitoring body verifies that the CSP complies with those requirements of the Code not covered by the third party reports.

LEVEL 3

Level 3 demonstrates compliance with every requirement outlined within the Code from third party assessments, audits or certifications. The audit reports must be internationally recognized standards and should provide sufficient information for the monitoring body to determine that the Code requirements were met.

EU Cloud Code of Conduct



Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016	NIST SP 800-53	Cybercurity Framework
[6.1.A] The CSP shall apply appropriate information security measures according to the sensitivity of the Customer Personal Data contained within the Cloud Service, considering a dedicated data protection assessment perspective when assessing the appropriateness of such measures.	[6.1.A] CSP should implement appropriate organizational and technical controls to secure data from ▪ accidental or unlawful destruction, ▪ loss, ▪ alteration, ▪ unauthorised disclosure of, or ▪ access to Customer Personal Data transmitted, stored or otherwise processed.	Art. 28.3 (c), Art. 28.3 (f)	A.8.2 Information classification A.5 Information security policies	A.8.2.2 Labelling of information	5.1.1 Policies for information security 8.2 Information classification	B.8.4 Privacy by design and privacy by default	C1.1 A1.1	SIM-02 Classification of Customer systems AM-05 Classification of information AM-06 Labelling of information and handling of assets	Access publicly available PDF version: NIST SP 800-53 AC-16 – Security and Privacy Attributes PE-19 – Information Leakage PM-5 – System Inventory PT-1 – Policies and Procedures	ID.AM: Asset Management ID.AM-1 ID-AM-2 ID-AM-3 ID.AM-4 PR.AC: Identity Management. Authentication, and Access Control PR.AC-1

EU Cloud Code of Conduct

How is the code monitored?

The monitoring body, Scope Europe, has the discretion to determine the final level of compliance based on the information provided by the CSP. Compliance with the Code is required every 12 months or sooner if significant changes occur or is a complaint is filed. While demonstration with the entire Code may not be required every 12 months, the CSP is required to maintain compliance at all times.

Europrivacy Certification Value Add

1. Legally recognized by all EU Member States
2. Identifies and reduces legal and financial risks
3. Assesses, validates and communicates compliance
4. Builds Trust and Confidence and improves reputation
5. Develops competitive advantages and market access
6. Saves control costs thanks to certified data processors
7. Turns data protection into an asset and source of revenues
8. Benefits from continuous compliance updates
9. Extends compliance to non-EU jurisdictions

Europrivacy™/®

Criteria to be Leveraged for Europrivacy Certification

The Europrivacy GDPR core criteria enable to assess compliance with regards to:

- Lawfulness of Data Processing
- Special Data Processing
- Rights of the Data Subjects
- Data Controller Responsibility
- Data Processors (or sub Processors)
- Security of Processing and Data Protection by Design
- Management of Data Breaches
- Data Protection Impact Assessment (DPIA)
- Data Protection Officer (DPO)
- Transfers of personal data to third countries or international organisations

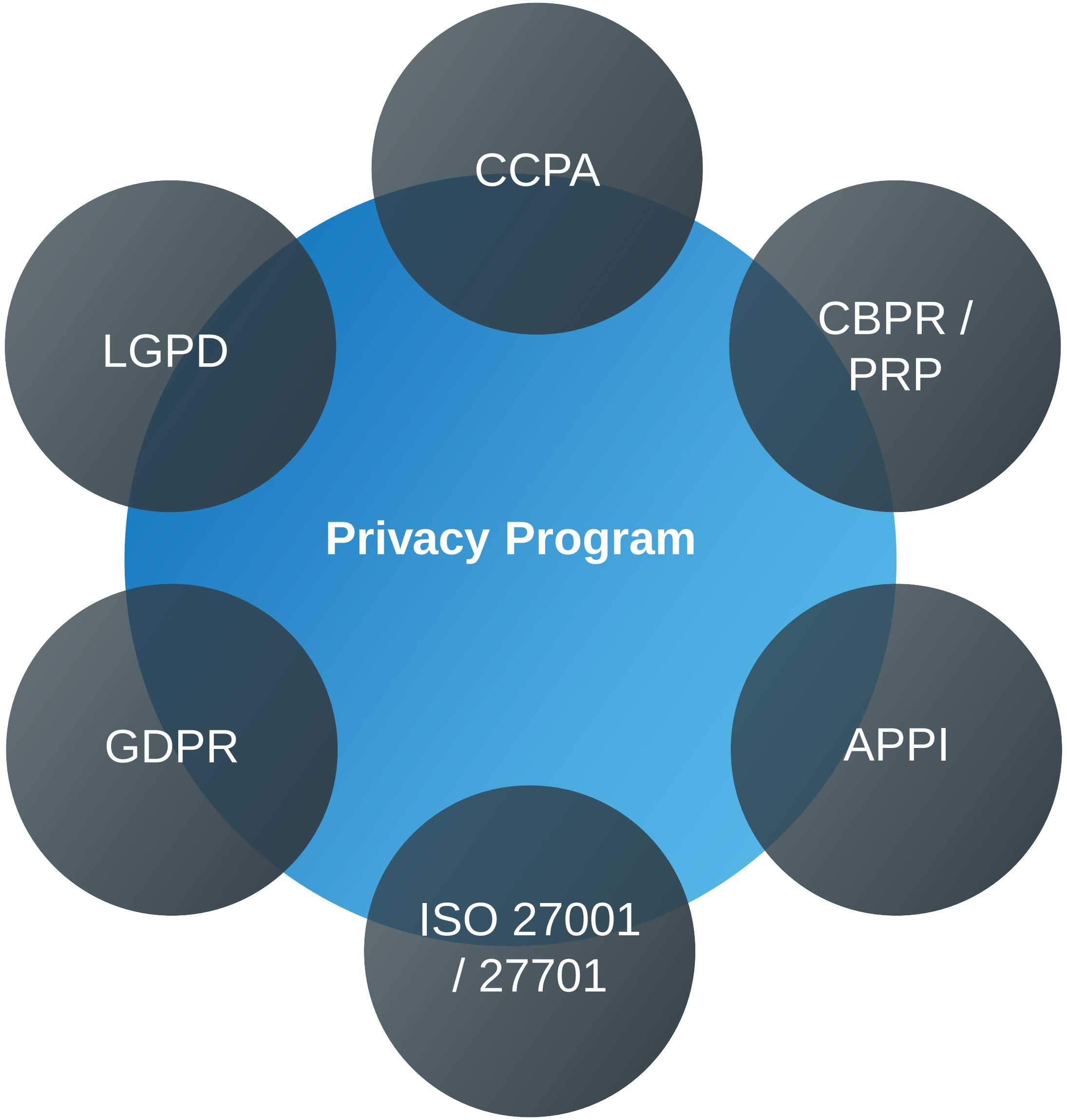
Where applicable, it is complemented by:

- Complementary Contextual Checks and Controls to assess technology and domain-specific obligations
- Technical and Organisational Measures (TOM) Checks and Controls to assess security requirements

Criteria to be Leveraged for New Frameworks/Regulations

Many of the organization’s existing privacy compliance efforts can be leveraged to meet new frameworks and regulations. Even if the requirements are not a 1:1 match, the underlying process and controls can be tweaked to get the organization the rest of the way there.

GOOD NEWS: If your organization has already implemented a privacy program, you are not starting from scratch.



Cross Border Privacy Rules & Privacy Recognition for Processors

There are two systems that were originally agreed upon by APEC economies, the **Cross-Border Privacy Rules(CBPR)** and the **Privacy Recognition for Processors (PRP)**. The systems approach privacy from a controller and processor perspective, respectively.

There are currently nine jurisdictions participating in the CBPR system, including:

- USA
- Mexico
- Japan
- Canada
- Singapore
- The Republic of Korea
- Australia
- Chinese Taipei
- Philippines

The systems are overseen by the Joint Oversight Panel (JOP), but enforcement is a joint operation, with local enforcement authorities playing a key role (FTC for the US).

The system seeks to provide a baseline of privacy considerations for all jurisdictions involved and allows for further requirements in member jurisdictions.

ISACA Chicago Chapter

Polling Question 3

What is a major benefit of including ISO/IEC 27701 in your existing ISO/IEC 27001 certification?

a) Comprehensive approach to privacy program

b) Flexible control structure for organizations operating in numerous jurisdictions

c) Good overlap with other privacy frameworks and regulations

d) All of the above

5

Q&A

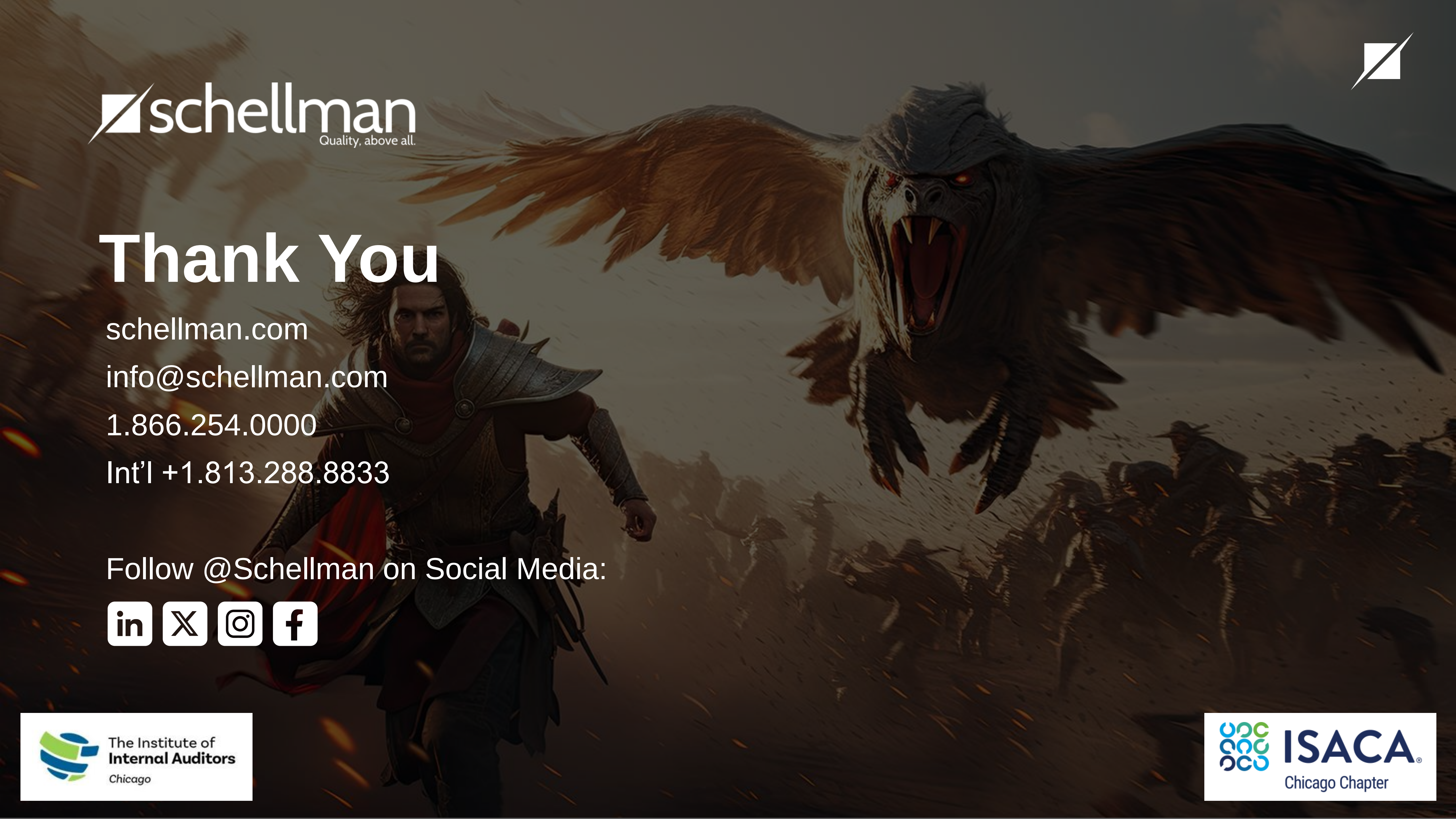
Questions

Welcome To The 10th Annual Hacking Conference

Remember to check-in to this session on the app!

The Institute of Internal Auditors
Chicago

ISACA
Chicago Chapter



schellman
Quality, above all.

Thank You

schellman.com
info@schellman.com
1.866.254.0000
Int’l +1.813.288.8833

Follow @Schellman on Social Media:

The Institute of Internal Auditors
Chicago

ISACA
Chicago Chapter