RMISC
ROCKY MOUNTAIN
INFORMATION SECURITY CONFERENCE

Tools and Techniques Using ISO Standards

ISO 27701 – Privacy Information Management Requirements

Tim Weil – ISO 27001/27701 Auditor/Trainer
Cybersecurity and Privacy Professional
SecurityFeeds (Denver)

Rocky Mountain Information Security Conference
Denver, CO Sept 28th, 2022

SecurityFeeds
Yor source for enterprise security management

Objectives of this Presentation

Top Privacy Risks in the Cloud

-- A Risk Management Dilemma

-- Risk Management Models

-- Data Breaches

-- Industry Look at Cloud Privacy Mandates

Top Privacy Threats in the Cloud

-- Pandemic Threat Study

-- Privacy Control Models (ISO 27018, CSA CCM 4.0)

-- Big Scary Monsters

ISO Standards for Cloud Security and Privacy

-- ISO 27001 (Information Security Management System)

-- ISO 27002 (27001 Annex A Control Sections)

-- ISO 27018 (Protecting PII in the Public Cloud)

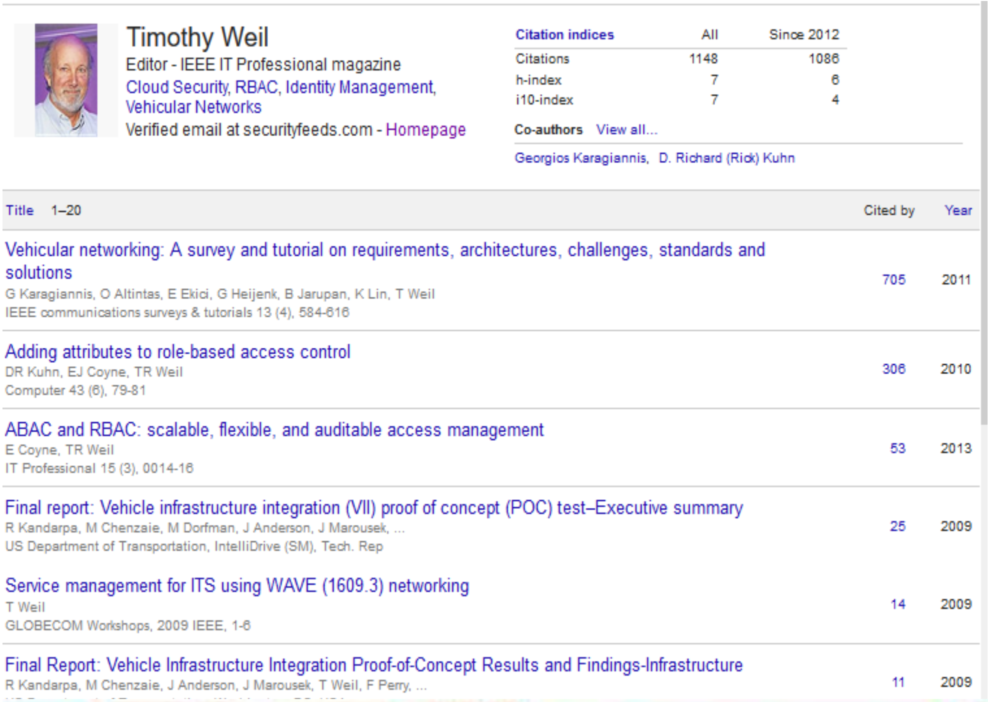
Tools & Techniques for PIMS Audits

-- Sample PIMS Audit

-- Methods

-- Requirements for PII Controllers, Principals and Processors

A Writer's Life –



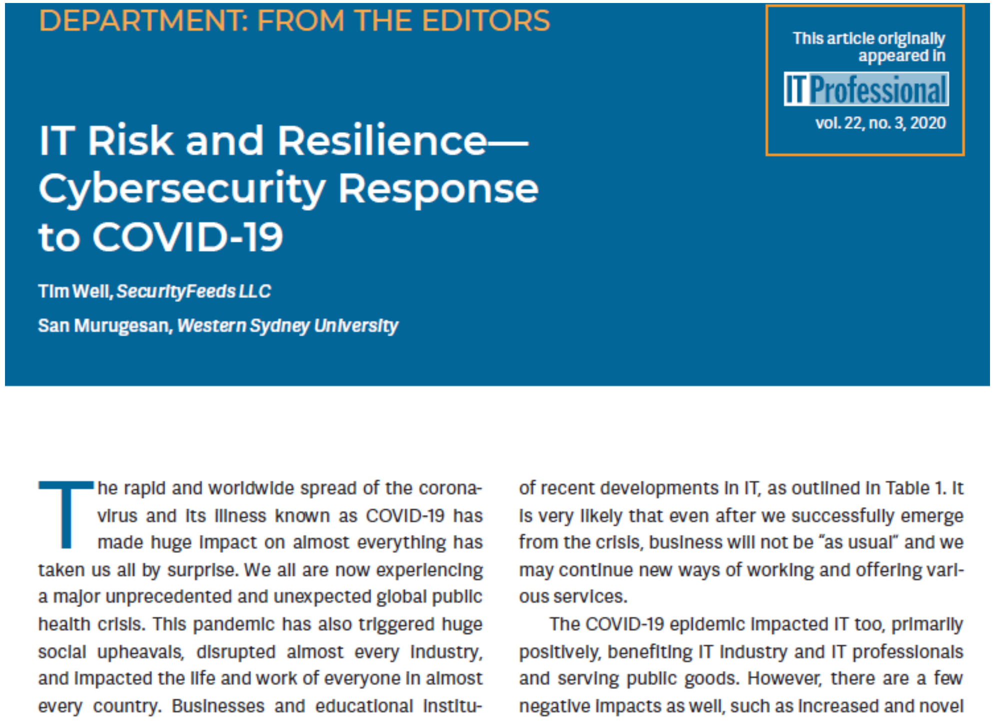
Timothy Weil
Editor - IEEE IT Professional magazine
Cloud Security, RBAC, Identity Management, Vehicular Networks
Verified email at securityfeeds.com - Homepage

Citation indices	All	Since 2012
Citations	1148	1086
h-index	7	6
i10-index	7	4

Co-authors View all...

Georgios Karagiannis, D. Richard (Rick) Kuhn

Title 1–20	Cited by	Year
Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions G Karagiannis, O Altintas, E Ekici, G Heijenk, B Jarupan, K Lin, T Weil IEEE communications surveys & tutorials 13 (4), 584-616	705	2011
Adding attributes to role-based access control DR Kuhn, EJ Coyne, TR Weil Computer 43 (6), 79-81	306	2010
ABAC and RBAC: scalable, flexible, and auditable access management E Coyne, TR Weil IT Professional 15 (3), 0014-16	53	2013
Final report: Vehicle infrastructure integration (VII) proof of concept (POC) test–Executive summary R Kandarpa, M Chenzaie, M Dorfman, J Anderson, J Marousek, ... US Department of Transportation, IntelliDrive (SM), Tech. Rep	25	2009
Service management for ITS using WAVE (1609.3) networking T Weil GLOBECOM Workshops, 2009 IEEE, 1-6	14	2009
Final Report: Vehicle Infrastructure Integration Proof-of-Concept Results and Findings-Infrastructure R Kandarpa, M Chenzaie, J Anderson, J Marousek, T Weil, F Perry, ...	11	2009



DEPARTMENT: FROM THE EDITORS

This article originally appeared in IT Professional vol. 22, no. 3, 2020

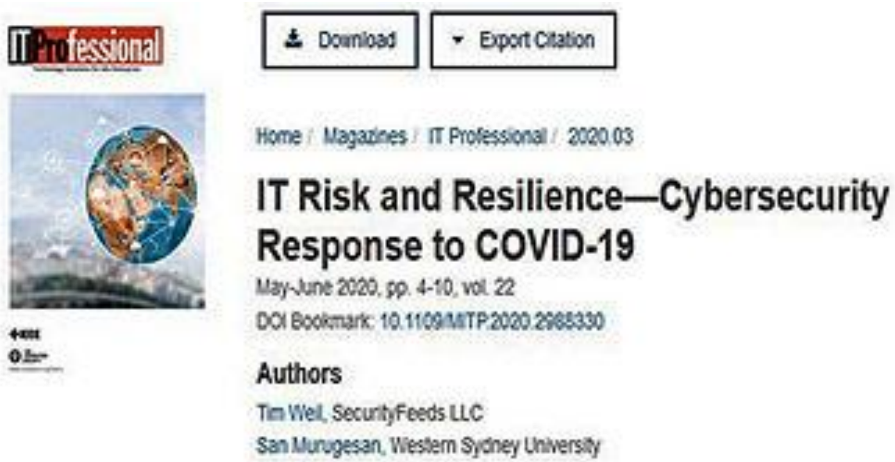
IT Risk and Resilience—Cybersecurity Response to COVID-19

Tim Weil, SecurityFeeds LLC
San Murugesan, Western Sydney University

The rapid and worldwide spread of the coronavirus and its illness known as COVID-19 has made huge impact on almost everything has taken us all by surprise. We all are now experiencing a major unprecedented and unexpected global public health crisis. This pandemic has also triggered huge social upheavals, disrupted almost every industry, and impacted the life and work of everyone in almost every country. Businesses and educational institu-

of recent developments in IT, as outlined in Table 1. It is very likely that even after we successfully emerge from the crisis, business will not be "as usual" and we may continue new ways of working and offering various services.

The COVID-19 epidemic impacted IT too, primarily positively, benefiting IT industry and IT professionals and serving public goods. However, there are a few negative impacts as well, such as increased and novel



Home / Magazines / IT Professional / 2020.03

IT Risk and Resilience—Cybersecurity Response to COVID-19

May-June 2020, pp. 4-10, vol. 22

DOI Bookmark: 10.1109/MITP.2020.2988330

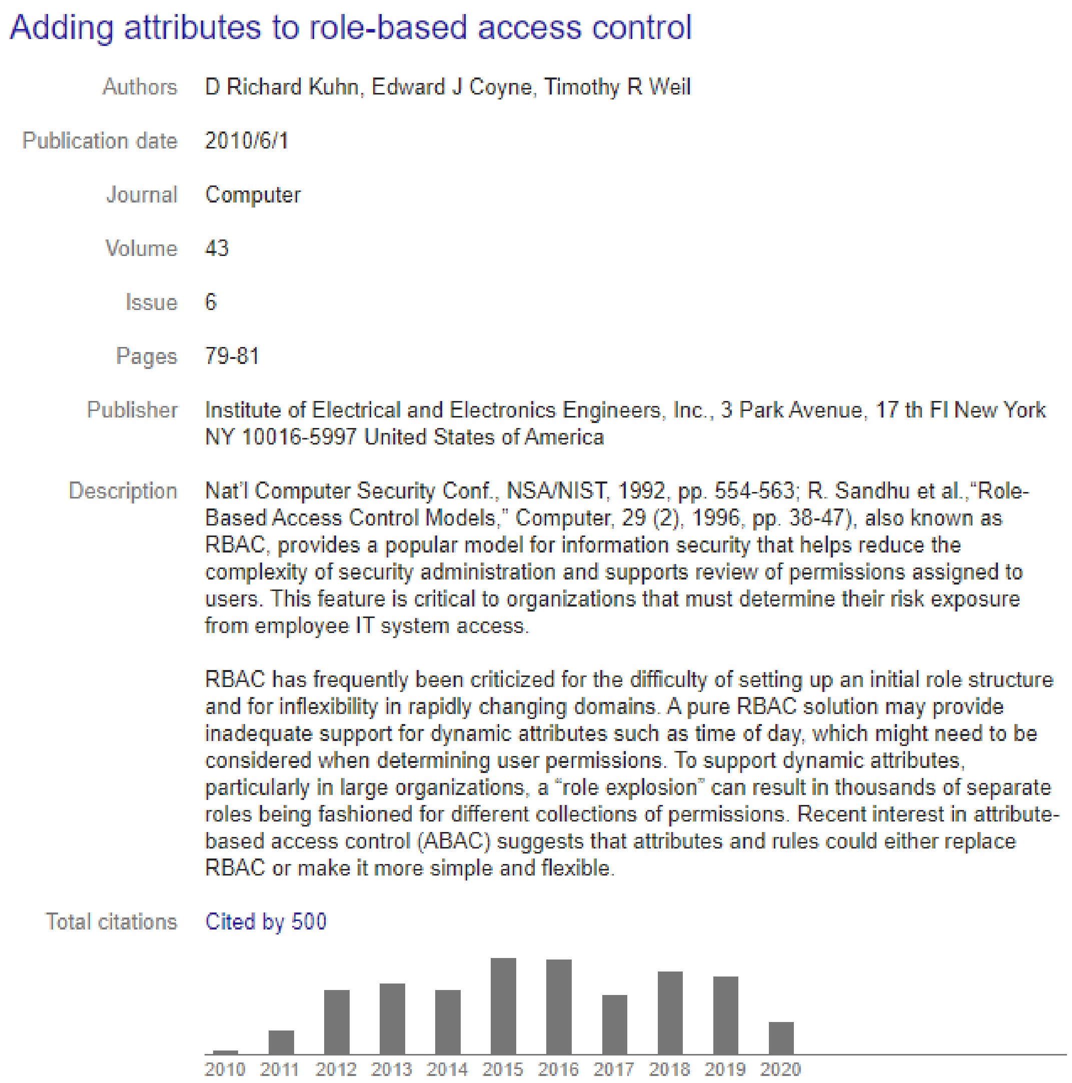
Authors

Tim Weil, SecurityFeeds LLC

San Murugesan, Western Sydney University

INFORMATION SECURITY CONFERENCE

Adding Attributes to Role Based Access Control reaches 500 citations on Google Scholar - https://lnkd.in/ew_BQaF



Adding attributes to role-based access control

Authors D Richard Kuhn, Edward J Coyne, Timothy R Weil

Publication date 2010/6/1

Journal Computer

Volume 43

Issue 6

Pages 79-81

Publisher Institute of Electrical and Electronics Engineers, Inc., 3 Park Avenue, 17 th Fl New York NY 10016-5997 United States of America

Description Nat'l Computer Security Conf., NSA/NIST, 1992, pp. 554-563; R. Sandhu et al.,"Role-Based Access Control Models," Computer, 29 (2), 1996, pp. 38-47), also known as RBAC, provides a popular model for information security that helps reduce the complexity of security administration and supports review of permissions assigned to users. This feature is critical to organizations that must determine their risk exposure from employee IT system access.

RBAC has frequently been criticized for the difficulty of setting up an initial role structure and for inflexibility in rapidly changing domains. A pure RBAC solution may provide inadequate support for dynamic attributes such as time of day, which might need to be considered when determining user permissions. To support dynamic attributes, particularly in large organizations, a "role explosion" can result in thousands of separate roles being fashioned for different collections of permissions. Recent interest in attribute-based access control (ABAC) suggests that attributes and rules could either replace RBAC or make it more simple and flexible.

Total citations Cited by 500

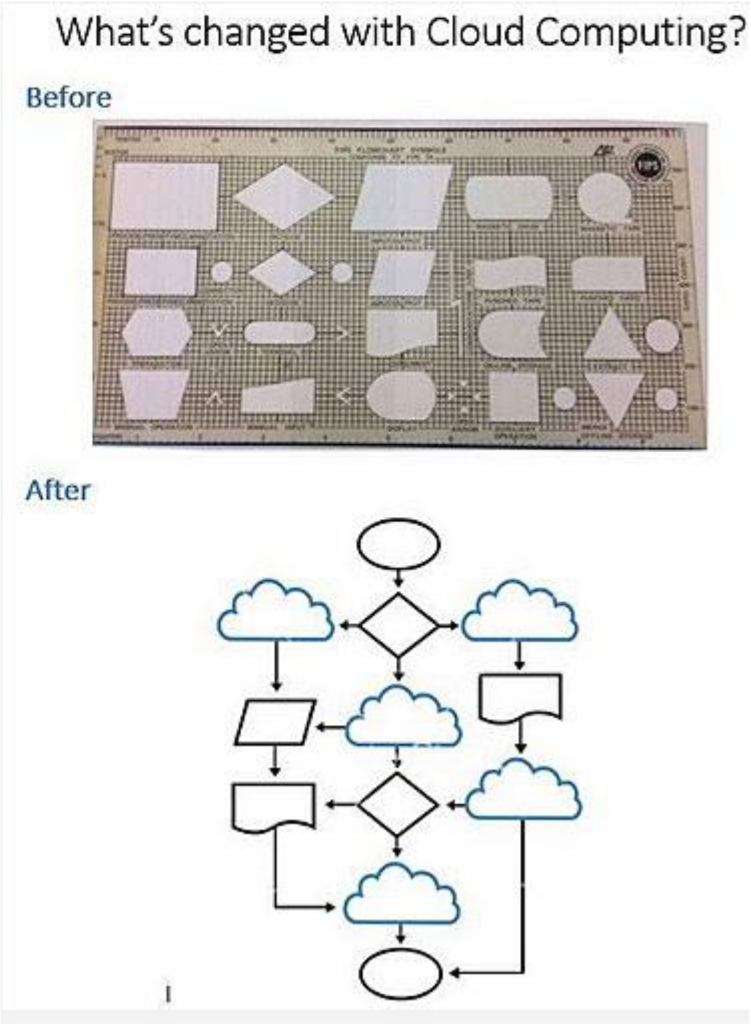
Table of Contents

- What are the Privacy Risks in the Age of Cloud Computing?
- Top Privacy Threats in the Cloud
- ISO Standards for Cloud Security and Privacy
- Tools and Techniques for PIMS Audits (ISO 27701)
- References + Q&A

How we got to the cloud

A look at the people, policies and technologies that have transformed federal IT in the past 25 years

The evolution of federal IT

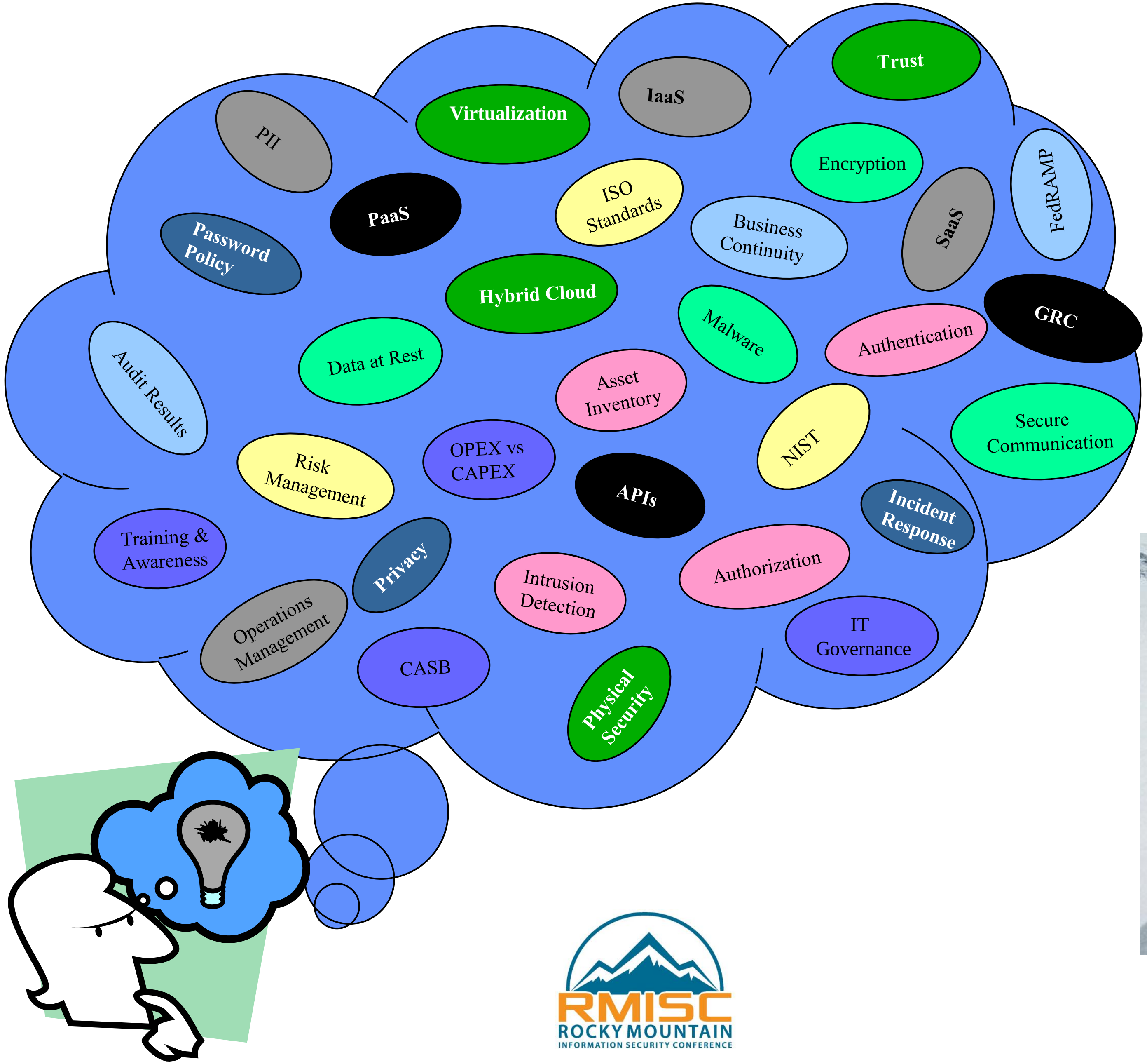


What's changed with Cloud Computing?

Before

After

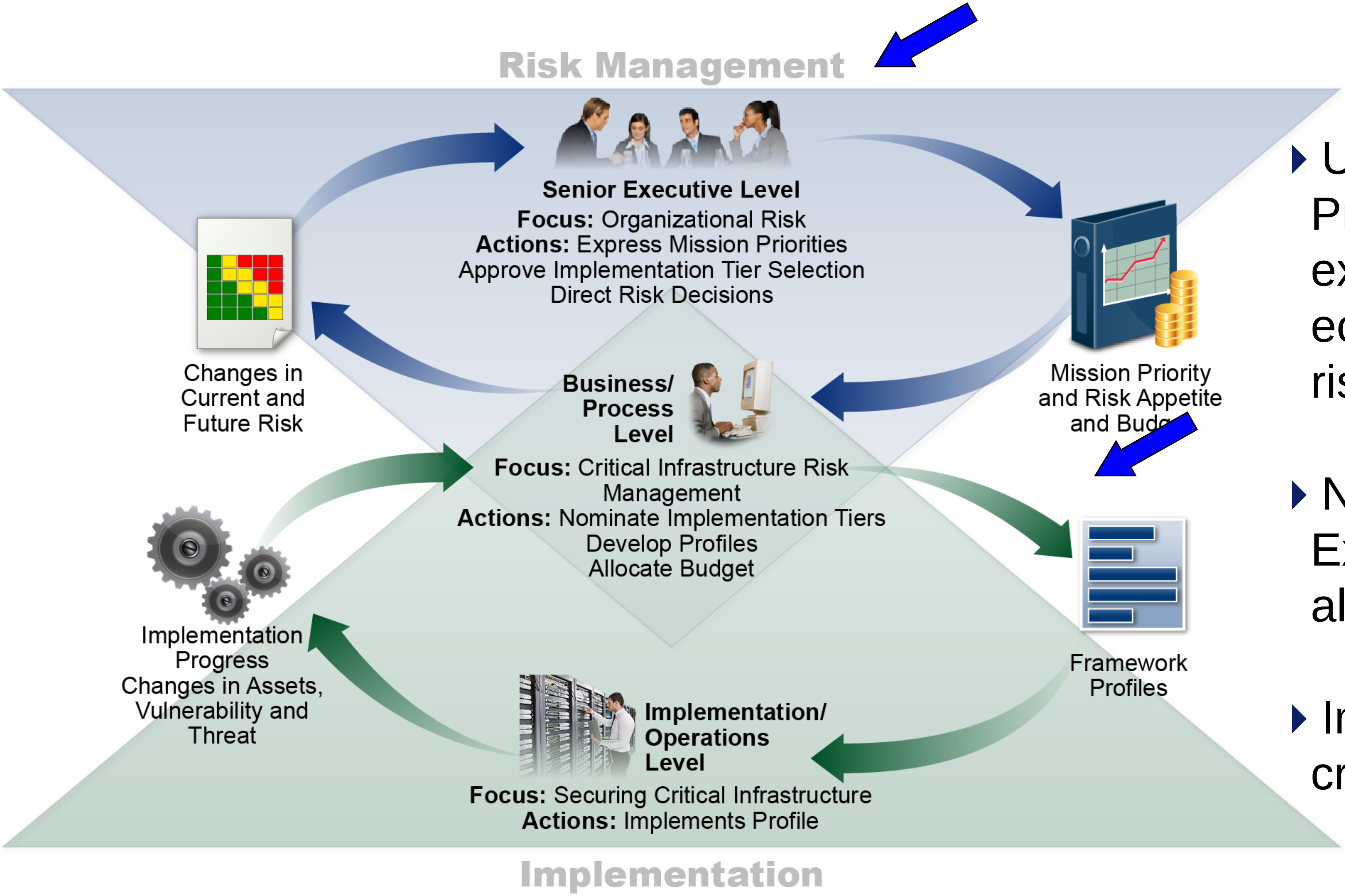
Now What? (Lessons learn from Enterprise Risk Assessment of the National Science Foundation’s US Antarctic Program)



Trust
IaaS
Virtualization
PII
Encryption
FedRAMP
ISO Standards
PaaS
Business Continuity
SaaS
Password Policy
Hybrid Cloud
Malware
Authentication
GRC
Audit Results
Data at Rest
Asset Inventory
Secure Communication
NIST
OPEX vs CAPEX
Risk Management
APIs
Incident Response
Training & Awareness
Privacy
Intrusion Detection
Authorization
Operations Management
CASB
IT Governance
Physical Security

IT 101 – What Problems Are We Trying to Solve?

- Identify ‘Fix-It’ areas in the program
- Understand Current State (Remediation)
- Improve ‘ad hoc’, ‘not my problem’ state
- **Manage Information Security & Privacy Risk**
- Improve Continuous Monitoring Process



Risk Management

Senior Executive Level
Focus: Organizational Risk
Actions: Express Mission Priorities
Approve Implementation Tier Selection
Direct Risk Decisions

Mission Priority
and Risk Appetite
and Budg

Changes in
Current and
Future Risk

Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Nominate Implementation Tiers
Develop Profiles
Allocate Budget

Framework
Profiles

Implementation
Progress
Changes in Assets,
Vulnerability and
Threat

Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile

Implementation

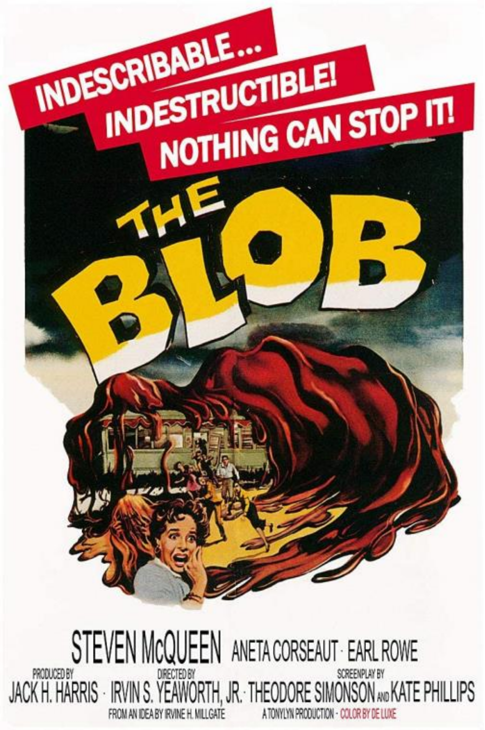
https://www.ssh.com/compliance/cybersecurity-framework/

- Use Risk Matrix to Prioritize actions and expenditures. Most economic value for eac risk considered.

- Nominate Tasks and Expenditures for budge allocation

- Implementation of critical Infrastructure

Big Scary Monsters - Global transformation caused by COVID-19

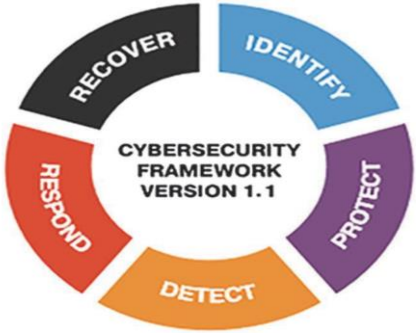

INDESCRIBABLE...
INDESTRUCTIBLE!
NOTHING CAN STOP IT!
THE BLOB
STEVEN McQUEEN ANETA CORSEAUT · EARL ROWE
PRODUCED BY JACK H. HARRIS · DIRECTED BY IRVIN S. YEAWORTH, JR. · SCREENPLAY BY THEODORE SIMONSON AND KATE PHILLIPS
FROM AN IDEA BY IRVINE H. MILLGATE
A TONYLYN PRODUCTION · COLOR BY DE LUXE

The Blob is an amorphous mass of alien goo that appears in the 1958 film of the same name. Appearing as nothing more than a mass of red gelatin, this creature possesses animalistic intelligence, acting purely on the instinct to feed. It feeds on flesh and gains mass as it consumes other creatures

A HORROR HORDE OF CRAWL-AND-CRUSH GIANTS
CLAWING OUT OF THE EARTH
FROM MILE-DEEP
CATACOMBS!
"THEM"
"This city is under martial law until we annihilate THEM!"
Kill one and two take it's place!
THE AMAZING NEW WARNER BROS. SENSATION!
"THEM!" JAMES WHITMORE . EDMUND GWENN . JOAN WELDON . JAMES ARNESS

Them While investigating a series of mysterious deaths, Sergeant Ben Peterson finds a young girl agent Robert Graham and scientist Dr. Harold Medford), he discovers that all the incidents are due to giant ants that have been mutated by atomic radiation. Peterson and Graham, with the aid of the military, attempt to find the queen ants and destroy the nests before the danger spreads.

The FUD Factor – Fear, Uncertainty and Doubt



CYBERSECURITY FRAMEWORK VERSION 1.1

IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER

Feeding the ‘Big Scary Monsters’ – PII Examples

Name

Address

Phone number

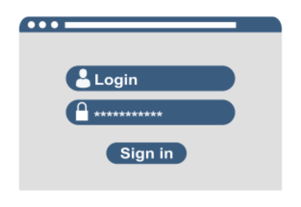
Email address

Date of birth

Marital status

Tax code

Bank details



Passwords

Driving licence

Passport number

Purchase history

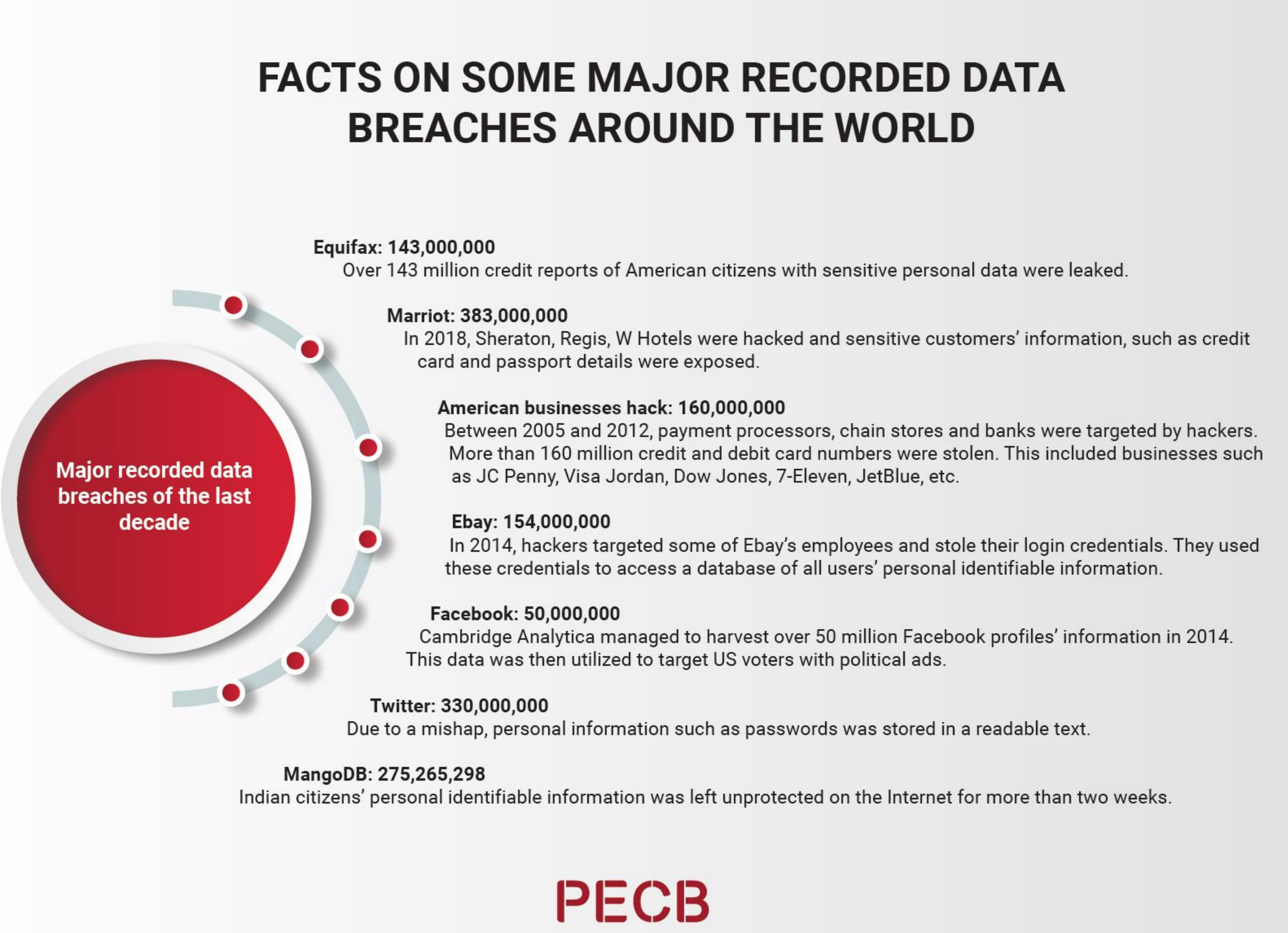
IP address

Mobile phone serial number

Special categories of PII

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health data
- Data concerning sex life
- Sexual orientation

Big Scary Monsters – Data Breaches



FACTS ON SOME MAJOR RECORDED DATA BREACHES AROUND THE WORLD

Major recorded data breaches of the last decade

Equifax: 143,000,000
Over 143 million credit reports of American citizens with sensitive personal data were leaked.

Marriot: 383,000,000
In 2018, Sheraton, Regis, W Hotels were hacked and sensitive customers' information, such as credit card and passport details were exposed.

American businesses hack: 160,000,000
Between 2005 and 2012, payment processors, chain stores and banks were targeted by hackers. More than 160 million credit and debit card numbers were stolen. This included businesses such as JC Penny, Visa Jordan, Dow Jones, 7-Eleven, JetBlue, etc.

Ebay: 154,000,000
In 2014, hackers targeted some of Ebay's employees and stole their login credentials. They used these credentials to access a database of all users' personal identifiable information.

Facebook: 50,000,000
Cambridge Analytica managed to harvest over 50 million Facebook profiles' information in 2014. This data was then utilized to target US voters with political ads.

Twitter: 330,000,000
Due to a mishap, personal information such as passwords was stored in a readable text.

MangoDB: 275,265,298
Indian citizens' personal identifiable information was left unprotected on the Internet for more than two weeks.

PECB

Managing Privacy Risk in the Cloud (Deloitte)-

Top Privacy Mitigations

- Understand and comply with various jurisdictional privacy laws
  - Where is your data stored?
  - EU General Protection Data Regulation(GDPR)
  - Canada Personal Information Protection and Electronic Documents Act (PIPEDA)

- How is you data protected?
  - Privacy by Design
  - Risk Assessment for ‘high risk’ data holdings

- How private is your data?
  - Data encryption mechanisms
  - Key management strategies

Deloitte.

Data privacy in the cloud
Navigating the new privacy regime in a cloud environment

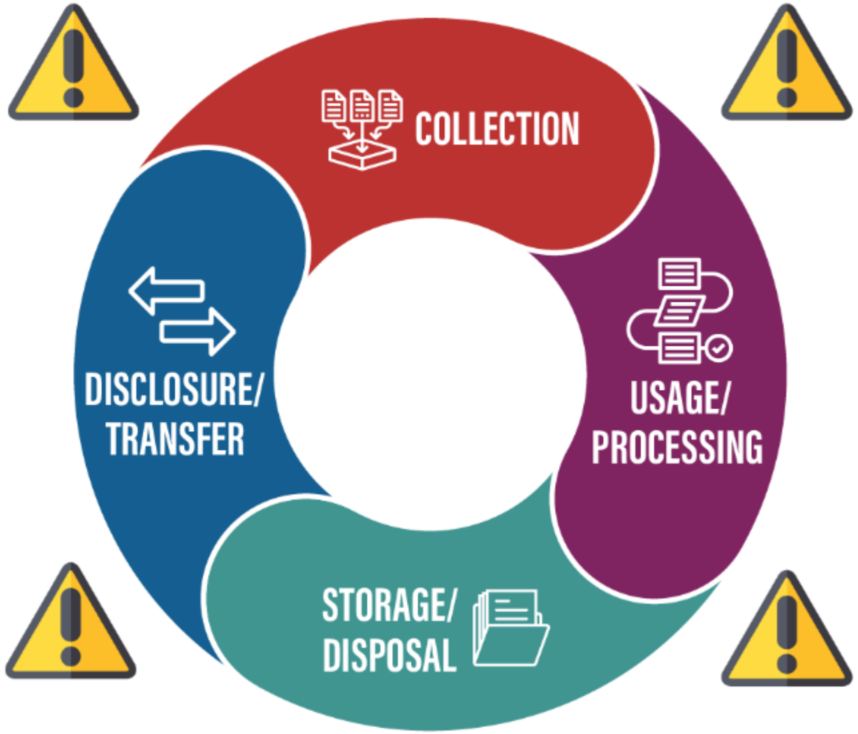
GDPR Requirements

- Mandatory Data Protection Officer
- Vendor and Partner Management
- Breach Notification
- Right to be Forgotten
- Data Portability
- Consent Management
- Fines for Non-Compliance
- Cross-Border Transfer

Privacy Risk in the Data Management Lifecycle

1. **Collection**
2. **Usage/Processing**
3. **Disclosure/Transfer**
4. **Storage/Disposal**

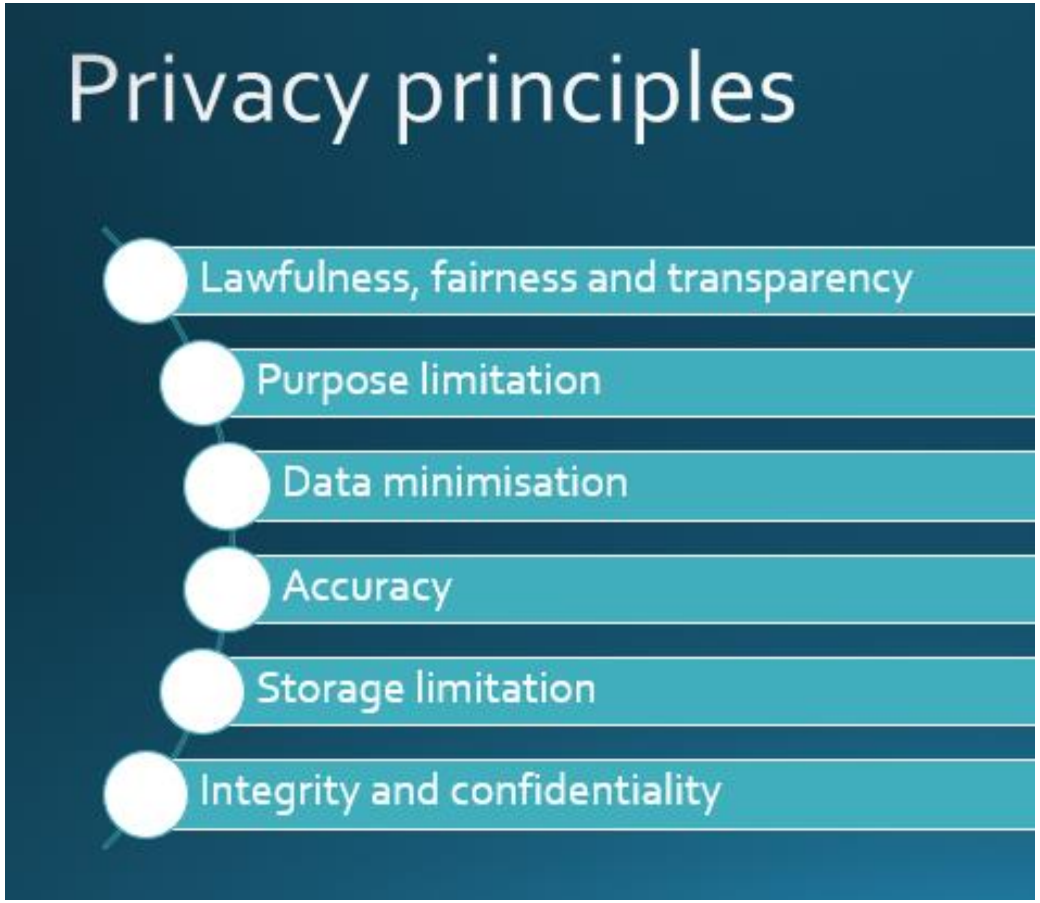
At every point, the organisation is subjected to the risk of exposures and breaches.



- To be able to address the various risks, business organizations need to implement a robust data protection management program including information security. The management of personal data within its lifecycle is a crucial step in the organization's efforts to ensure the privacy, confidentiality, availability and integrity of personally identifiable information.

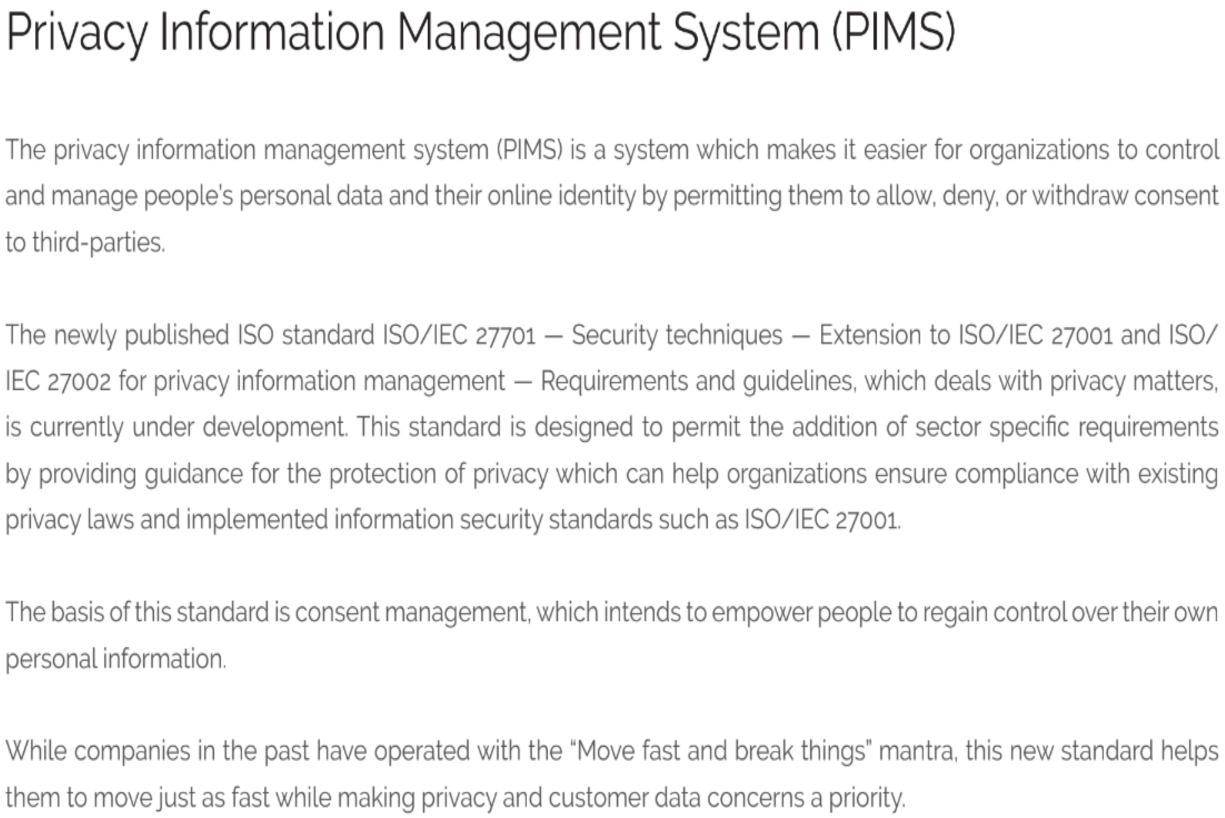
https://www.dpexnetwork.org/articles/benefits-implementing-isoiec-27701-privacy-information-management-system

Privacy Risk in the Data Management Lifecycle



Privacy principles

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality



Privacy Information Management System (PIMS)

The privacy information management system (PIMS) is a system which makes it easier for organizations to control and manage people's personal data and their online identity by permitting them to allow, deny, or withdraw consent to third-parties.

The newly published ISO standard ISO/IEC 27701 — Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines, which deals with privacy matters, is currently under development. This standard is designed to permit the addition of sector specific requirements by providing guidance for the protection of privacy which can help organizations ensure compliance with existing privacy laws and implemented information security standards such as ISO/IEC 27001.

The basis of this standard is consent management, which intends to empower people to regain control over their own personal information.

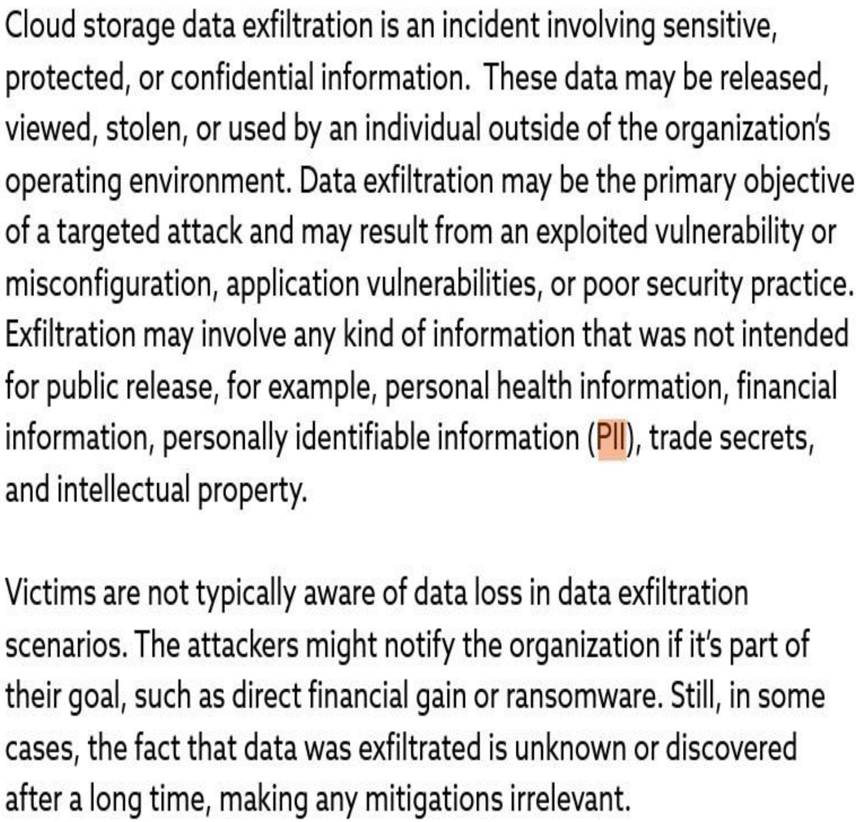
While companies in the past have operated with the "Move fast and break things" mantra, this new standard helps them to move just as fast while making privacy and customer data concerns a priority.

Table of Contents

- What are the Privacy Risks in the Age of Cloud Computing?
- Privacy Threats and Protection in the Cloud
- ISO Standards for Cloud Security and Privacy
- Tools and Techniques for PIMS Audits (ISO 27701)
- References + Q&A

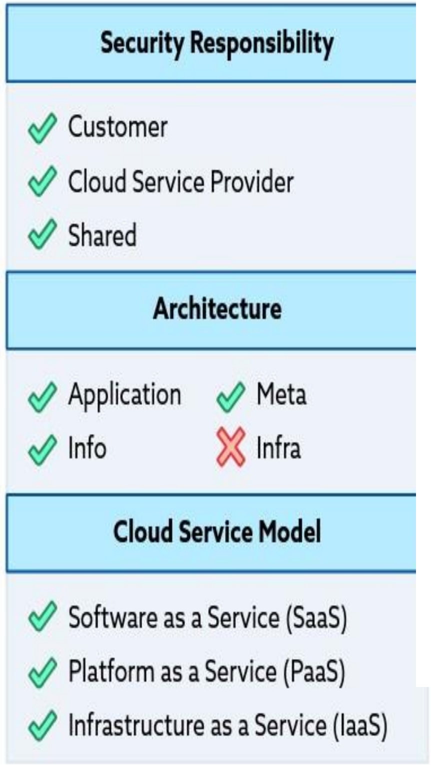
Cloud Security Alliance – Top Pandemic Threats

https://cloudsecurityalliance.org/



Cloud storage data exfiltration is an incident involving sensitive, protected, or confidential information. These data may be released, viewed, stolen, or used by an individual outside of the organization's operating environment. Data exfiltration may be the primary objective of a targeted attack and may result from an exploited vulnerability or misconfiguration, application vulnerabilities, or poor security practice. Exfiltration may involve any kind of information that was not intended for public release, for example, personal health information, financial information, personally identifiable information (PII), trade secrets, and intellectual property.

Victims are not typically aware of data loss in data exfiltration scenarios. The attackers might notify the organization if it's part of their goal, such as direct financial gain or ransomware. Still, in some cases, the fact that data was exfiltrated is unknown or discovered after a long time, making any mitigations irrelevant.



Security Responsibility

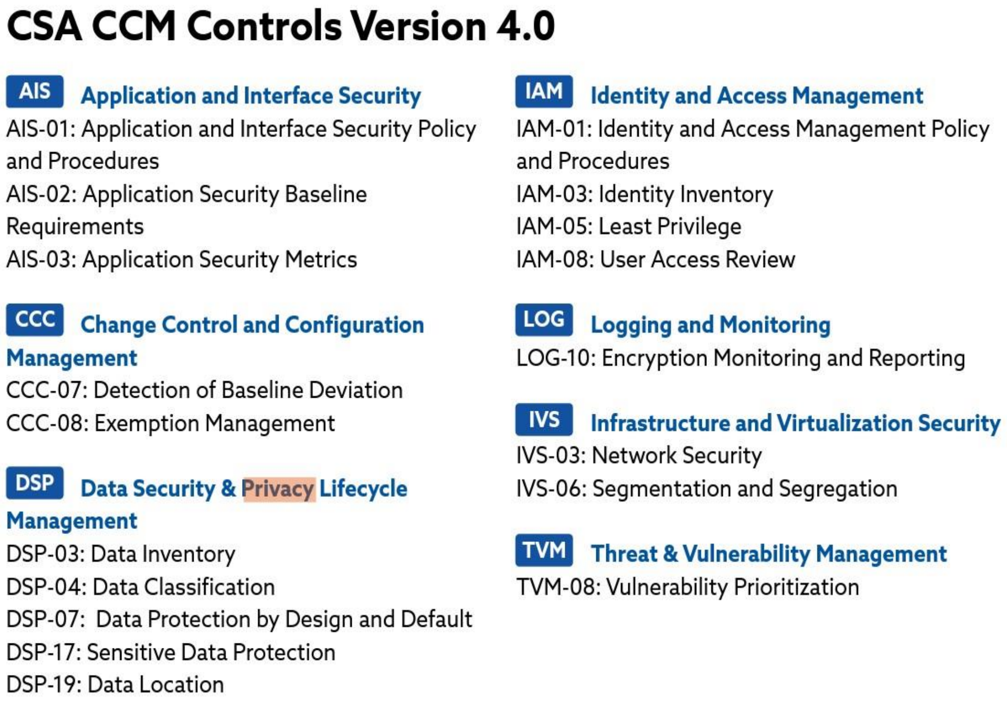
✓ Customer
✓ Cloud Service Provider
✓ Shared

Architecture

✓ Application ✓ Meta
✓ Info ✗ Infra

Cloud Service Model

✓ Software as a Service (SaaS)
✓ Platform as a Service (PaaS)
✓ Infrastructure as a Service (IaaS)



CSA CCM Controls Version 4.0

AIS Application and Interface Security
AIS-01: Application and Interface Security Policy and Procedures
AIS-02: Application Security Baseline Requirements
AIS-03: Application Security Metrics

CCC Change Control and Configuration Management
CCC-07: Detection of Baseline Deviation
CCC-08: Exemption Management

DSP Data Security & Privacy Lifecycle Management
DSP-03: Data Inventory
DSP-04: Data Classification
DSP-07: Data Protection by Design and Default
DSP-17: Sensitive Data Protection
DSP-19: Data Location

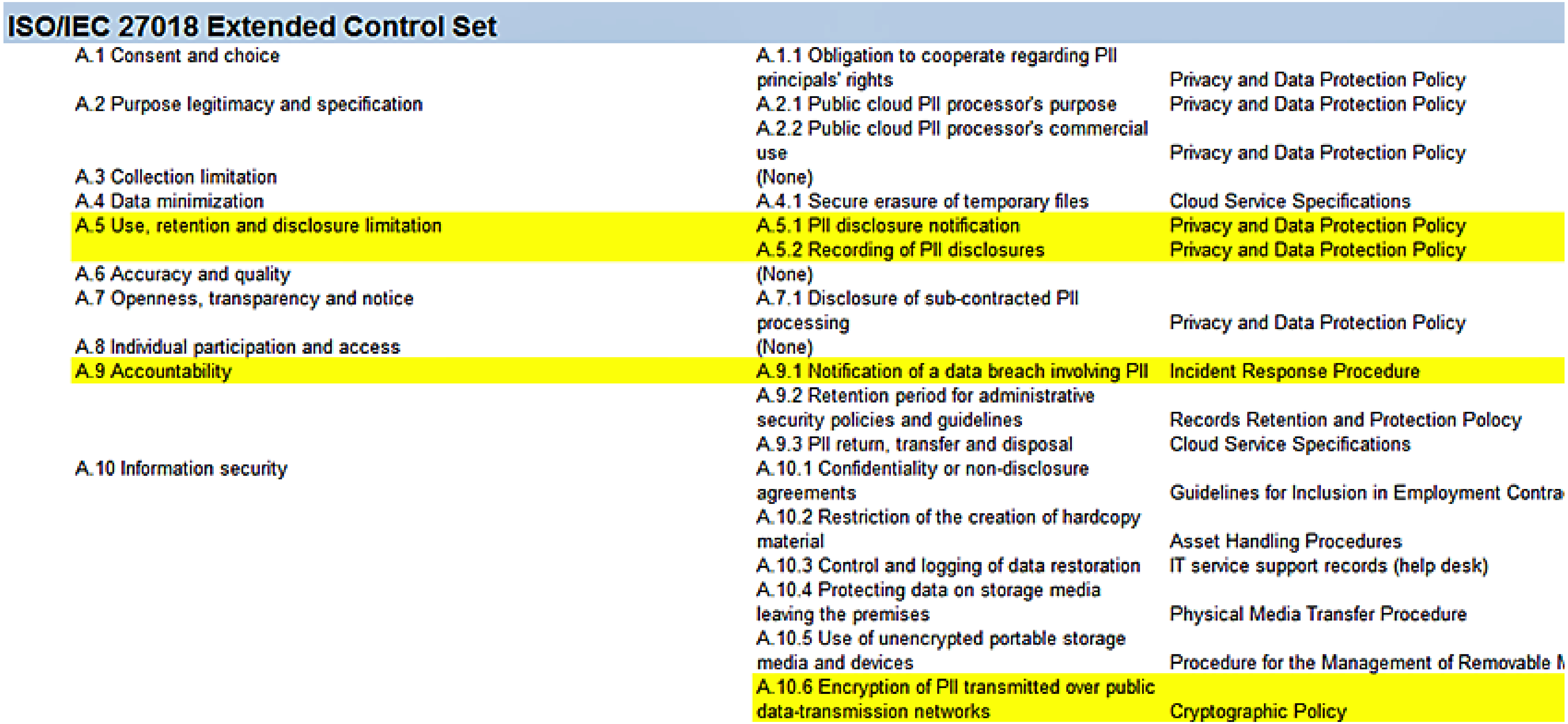
IAM Identity and Access Management
IAM-01: Identity and Access Management Policy and Procedures
IAM-03: Identity Inventory
IAM-05: Least Privilege
IAM-08: User Access Review

LOG Logging and Monitoring
LOG-10: Encryption Monitoring and Reporting

IVS Infrastructure and Virtualization Security
IVS-03: Network Security
IVS-06: Segmentation and Segregation

TVM Threat & Vulnerability Management
TVM-08: Vulnerability Prioritization

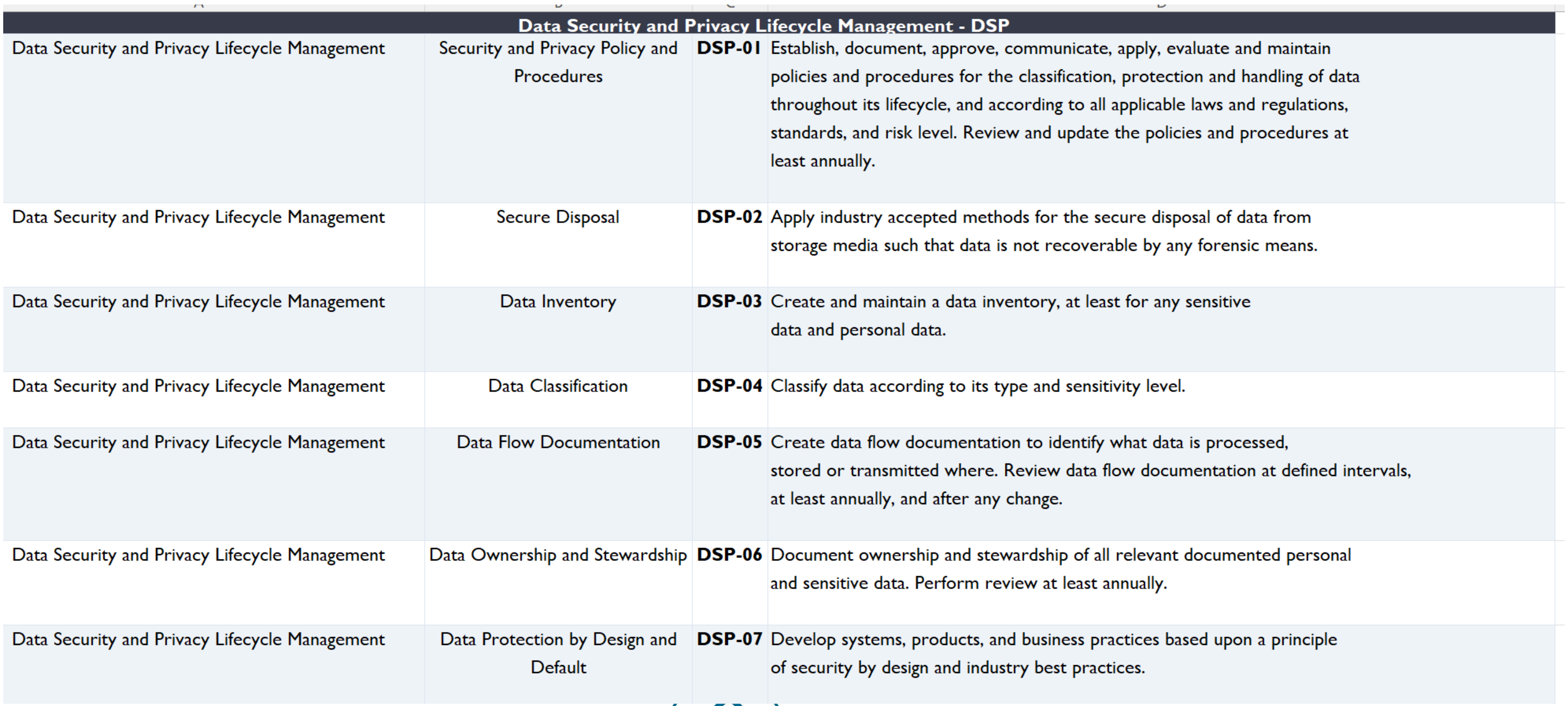
Protection of personally identifiable information (PII) in *public clouds* acting as PII processors – ISO 27018



ISO/IEC 27018 Extended Control Set

A.1 Consent and choice	A.1.1 Obligation to cooperate regarding PII principals' rights	Privacy and Data Protection Policy
A.2 Purpose legitimacy and specification	A.2.1 Public cloud PII processor's purpose	Privacy and Data Protection Policy
	A.2.2 Public cloud PII processor's commercial use	Privacy and Data Protection Policy
A.3 Collection limitation	(None)	
A.4 Data minimization	A.4.1 Secure erasure of temporary files	Cloud Service Specifications
A.5 Use, retention and disclosure limitation	A.5.1 PII disclosure notification	Privacy and Data Protection Policy
	A.5.2 Recording of PII disclosures	Privacy and Data Protection Policy
A.6 Accuracy and quality	(None)	
A.7 Openness, transparency and notice	A.7.1 Disclosure of sub-contracted PII processing	Privacy and Data Protection Policy
A.8 Individual participation and access	(None)	
A.9 Accountability	A.9.1 Notification of a data breach involving PII	Incident Response Procedure
	A.9.2 Retention period for administrative security policies and guidelines	Records Retention and Protection Polocy
	A.9.3 PII return, transfer and disposal	Cloud Service Specifications
A.10 Information security	A.10.1 Confidentiality or non-disclosure agreements	Guidelines for Inclusion in Employment Contra
	A.10.2 Restriction of the creation of hardcopy material	Asset Handling Procedures
	A.10.3 Control and logging of data restoration	IT service support records (help desk)
	A.10.4 Protecting data on storage media leaving the premises	Physical Media Transfer Procedure
	A.10.5 Use of unencrypted portable storage media and devices	Procedure for the Management of Removable
	A.10.6 Encryption of PII transmitted over public data-transmission networks	Cryptographic Policy

Cloud Security Alliance CCM4.0 –
Data Security and Privacy Lifecycle Management (18 Controls)

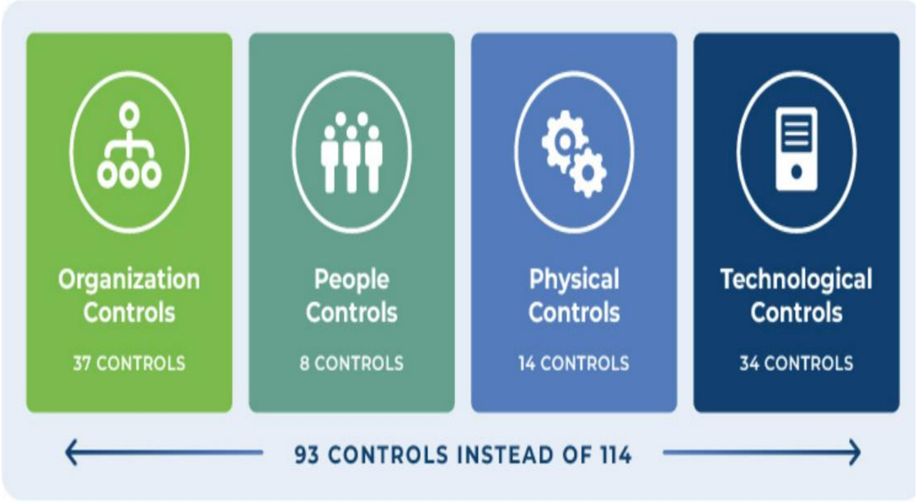


Data Security and Privacy Lifecycle Management - DSP

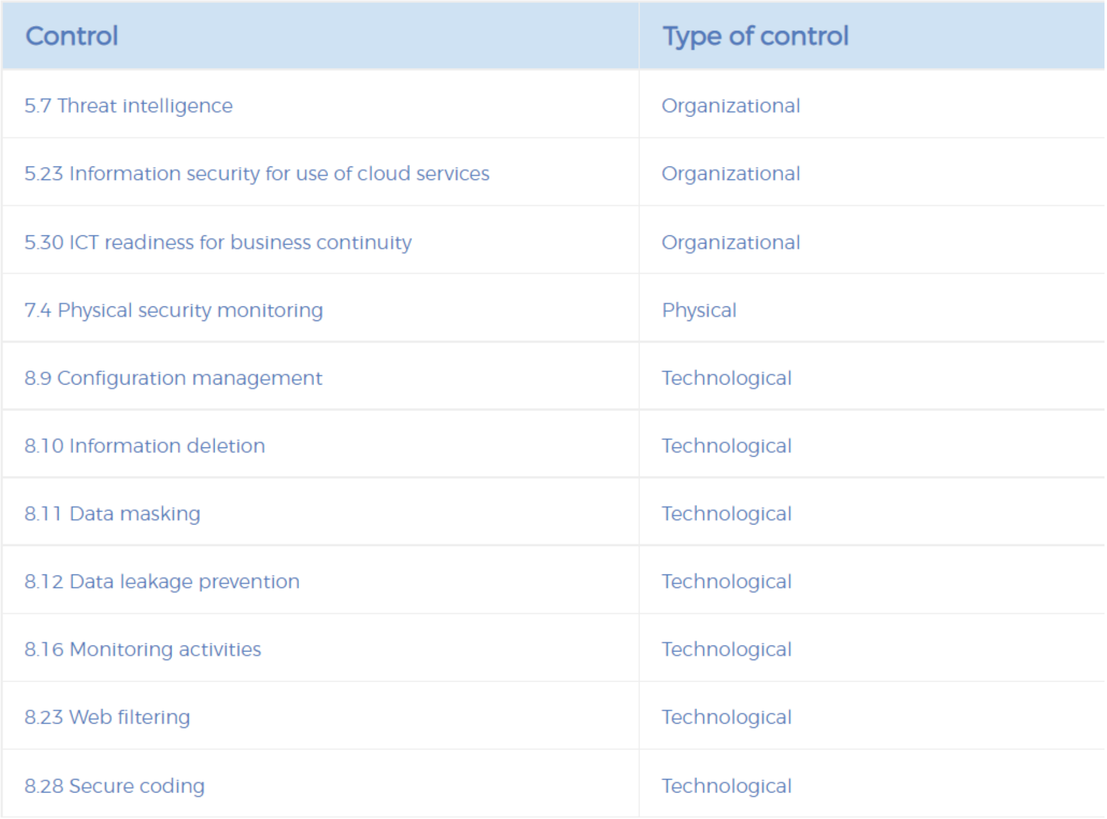
Data Security and Privacy Lifecycle Management	Security and Privacy Policy and Procedures	**DSP-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the classification, protection and handling of data throughout its lifecycle, and according to all applicable laws and regulations, standards, and risk level. Review and update the policies and procedures at least annually.
Data Security and Privacy Lifecycle Management	Secure Disposal	**DSP-02**	Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means.
Data Security and Privacy Lifecycle Management	Data Inventory	**DSP-03**	Create and maintain a data inventory, at least for any sensitive data and personal data.
Data Security and Privacy Lifecycle Management	Data Classification	**DSP-04**	Classify data according to its type and sensitivity level.
Data Security and Privacy Lifecycle Management	Data Flow Documentation	**DSP-05**	Create data flow documentation to identify what data is processed, stored or transmitted where. Review data flow documentation at defined intervals, at least annually, and after any change.
Data Security and Privacy Lifecycle Management	Data Ownership and Stewardship	**DSP-06**	Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually.
Data Security and Privacy Lifecycle Management	Data Protection by Design and Default	**DSP-07**	Develop systems, products, and business practices based upon a principle of security by design and industry best practices.

ISO 27002:2022 vs :2013

https://www.advantio.com/blog/whats-new-in-iso/iec-27002-2022-updates



To consolidate the increased number of controls in this version, 11 new controls have been added. Only 1 control from the previous version has been removed, and 57 controls that had similar objectives have been merged into 24 new controls.



Control	Type of control
5.7 Threat intelligence	Organizational
5.23 Information security for use of cloud services	Organizational
5.30 ICT readiness for business continuity	Organizational
7.4 Physical security monitoring	Physical
8.9 Configuration management	Technological
8.10 Information deletion	Technological
8.11 Data masking	Technological
8.12 Data leakage prevention	Technological
8.16 Monitoring activities	Technological
8.23 Web filtering	Technological
8.28 Secure coding	Technological

Table of Contents

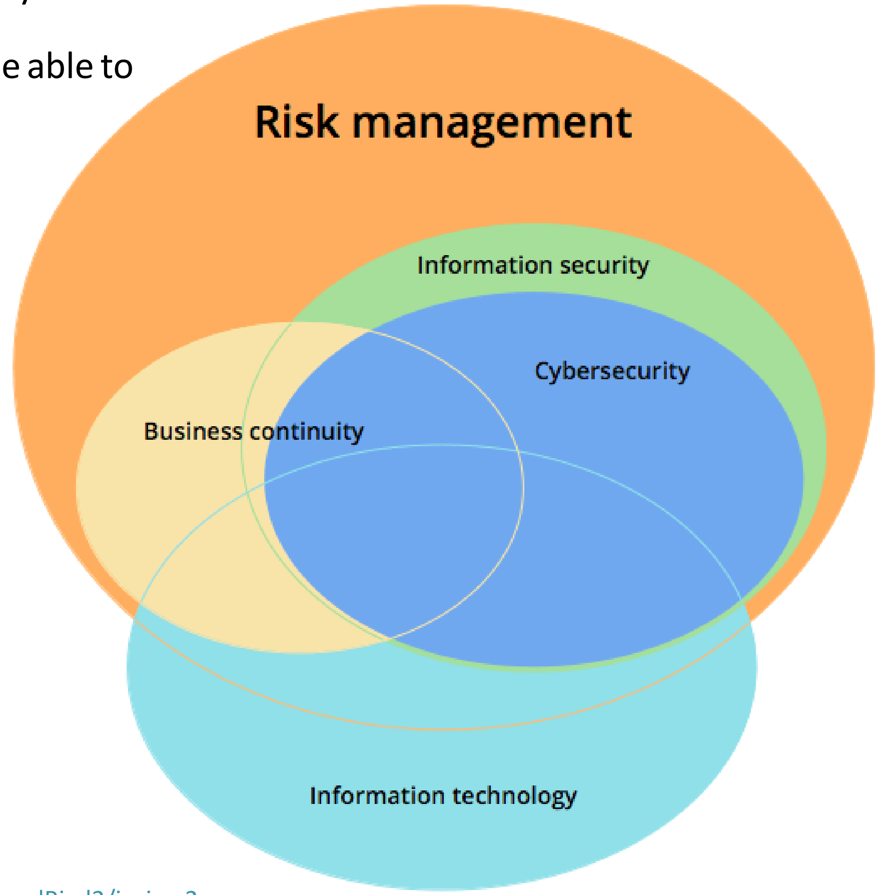
- What are the Privacy Risks in the Age of Cloud Computing?
- Privacy Threats and Protection in the Cloud
- ISO Standards for Cloud Security and Privacy
- ISO Tools and Techniques for PIMS Audits (ISO 27701)
- References + Q&A

Benefits of ISO 27001 - ISO /IEC 27001:2013 Structure and Content

ISO/IEC 27001:2013 Implementation, Certification from a certification body demonstrates that the security of organization information has been addressed, valuable data and information assets properly controlled.

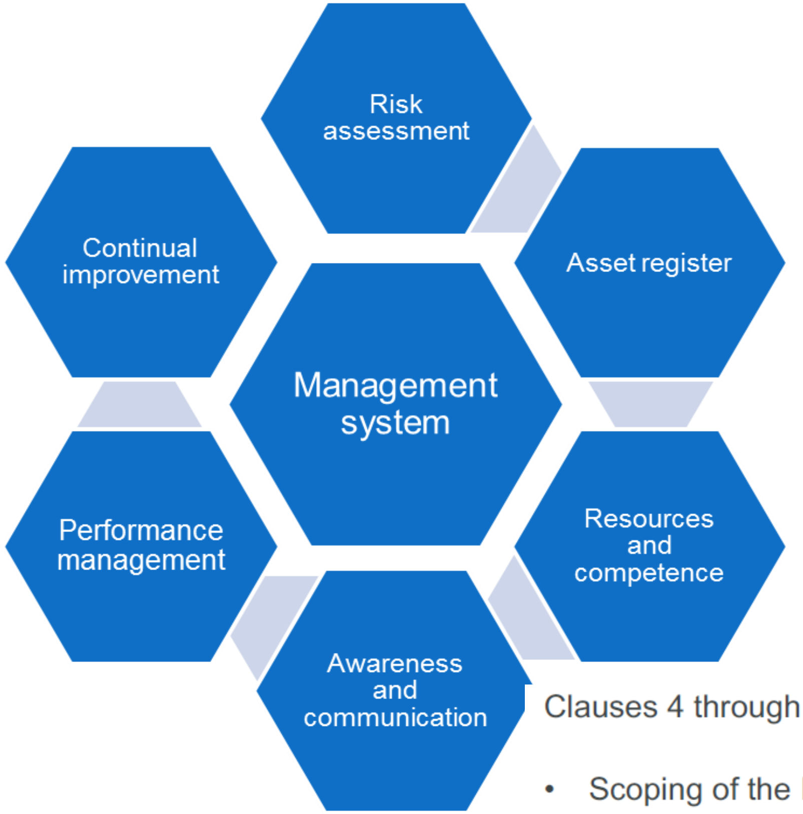
Also there is List of benefits By achieving certification to ISO/IEC 27001:2013 organization will be able to acquire numerous benefits including:

- Keeps confidential information secure
- Provides customers and stakeholders with confidence in how you manage risk
- Secure exchange of information
- Provide Organization with a competitive advantage
- Enhanced customer satisfaction
- Consistency in the delivery of your service or product
- Manages and minimises risk exposure
- Builds a culture of security
- Protects the Organization assets, shareholders and Customers
- Protects the company, assets, shareholders and directors



Ahmed Riad, BlueKaizen Magazine, Benefits of ISO 27001- https://www.slideshare.net/AhmedRiad2/isoiec-https://www.slideshare.net/AhmedRiad2/isoiec-2

The ISO/IEC 27001 standard



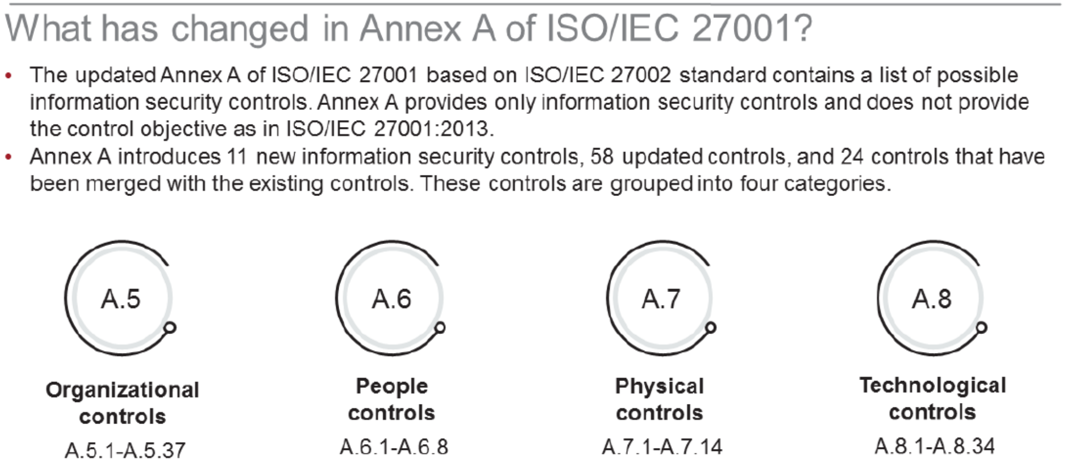
Clauses 4 through 10 deal with:

- Scoping of the ISMS
- Identifying and evaluating Risks
- Risk Treatment and mitigation
- Managing and measuring performance of the
- Tracking non-conformities and resolution
- Continuous improvement

Annex A deals with:
114 Optional controls for risk mitigation

ISO/IEC 27001 Controls v2022 vs 2013

Information security policies	Organisation of information security	Human resources security	Asset management
Access control	Cryptography	Physical and environmental security	Operations security
Communications security	System acquisition, development and maintenance	Supplier relationships	Incident management
	Business continuity management	Compliance	



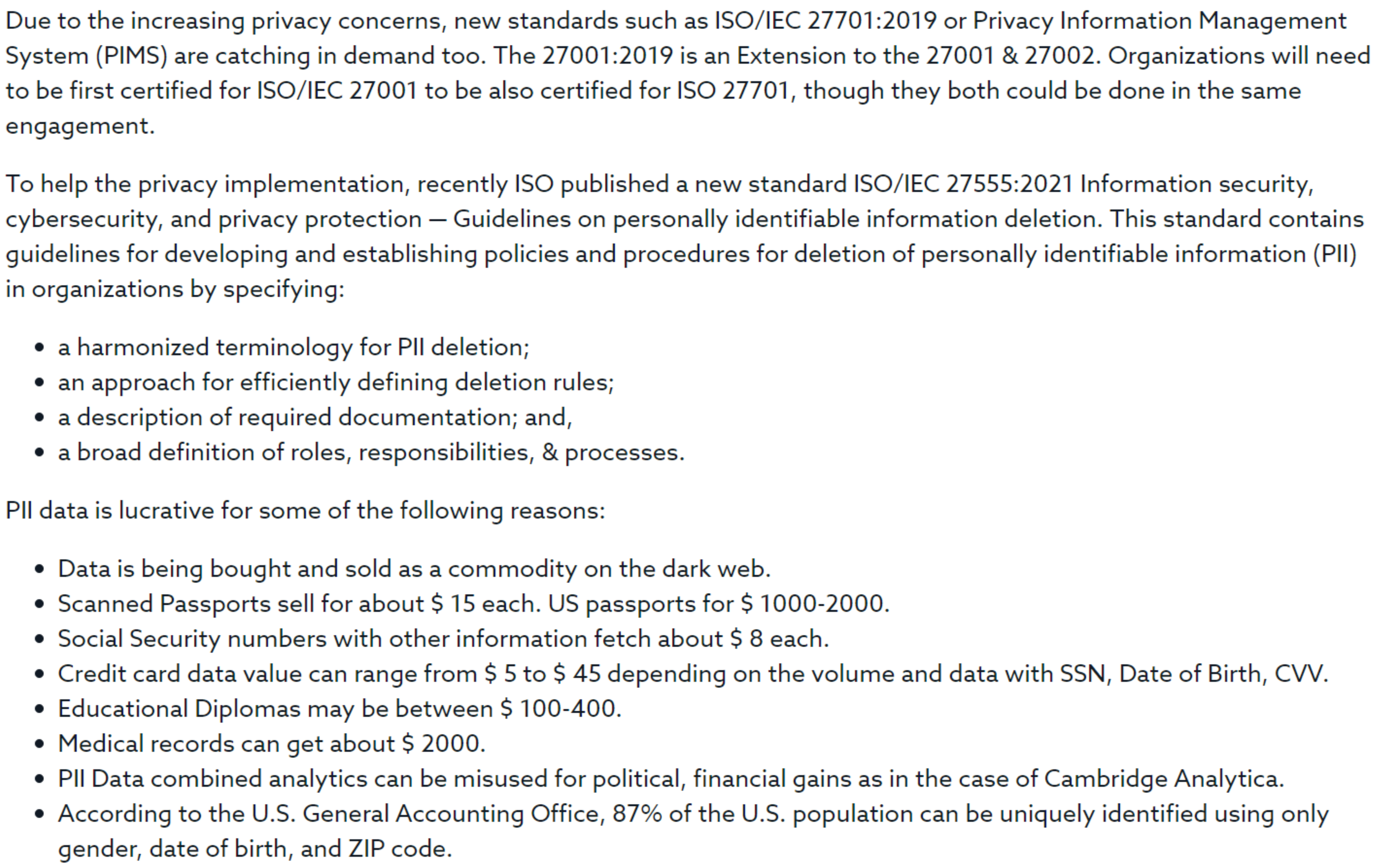
What has changed in Annex A of ISO/IEC 27001?

- The updated Annex A of ISO/IEC 27001 based on ISO/IEC 27002 standard contains a list of possible information security controls. Annex A provides only information security controls and does not provide the control objective as in ISO/IEC 27001:2013.
- Annex A introduces 11 new information security controls, 58 updated controls, and 24 controls that have been merged with the existing controls. These controls are grouped into four categories.

A.5	A.6	A.7	A.8
Organizational controls	**People controls**	**Physical controls**	**Technological controls**
A.5.1-A.5.37	A.6.1-A.6.8	A.7.1-A.7.14	A.8.1-A.8.34

ISO 27701 - Privacy Information Management System (PIMS)

https://cloudsecurityalliance.org/blog/2021/11/17/data-security-and-privacy-related-iso-iec-certifications/



Due to the increasing privacy concerns, new standards such as ISO/IEC 27701:2019 or Privacy Information Management System (PIMS) are catching in demand too. The 27001:2019 is an Extension to the 27001 & 27002. Organizations will need to be first certified for ISO/IEC 27001 to be also certified for ISO 27701, though they both could be done in the same engagement.

To help the privacy implementation, recently ISO published a new standard ISO/IEC 27555:2021 Information security, cybersecurity, and privacy protection — Guidelines on personally identifiable information deletion. This standard contains guidelines for developing and establishing policies and procedures for deletion of personally identifiable information (PII) in organizations by specifying:

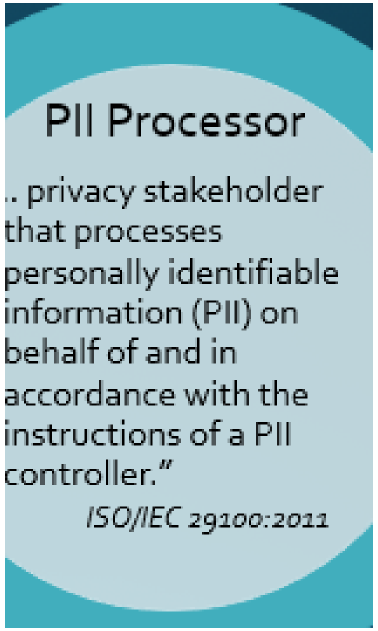
- a harmonized terminology for PII deletion;
- an approach for efficiently defining deletion rules;
- a description of required documentation; and,
- a broad definition of roles, responsibilities, & processes.

PII data is lucrative for some of the following reasons:

- Data is being bought and sold as a commodity on the dark web.
- Scanned Passports sell for about $ 15 each. US passports for $ 1000-2000.
- Social Security numbers with other information fetch about $ 8 each.
- Credit card data value can range from $ 5 to $ 45 depending on the volume and data with SSN, Date of Birth, CVV.
- Educational Diplomas may be between $ 100-400.
- Medical records can get about $ 2000.
- PII Data combined analytics can be misused for political, financial gains as in the case of Cambridge Analytica.
- According to the U.S. General Accounting Office, 87% of the U.S. population can be uniquely identified using only gender, date of birth, and ZIP code.

ISO 27701 - Privacy Information Management System (PIMS)

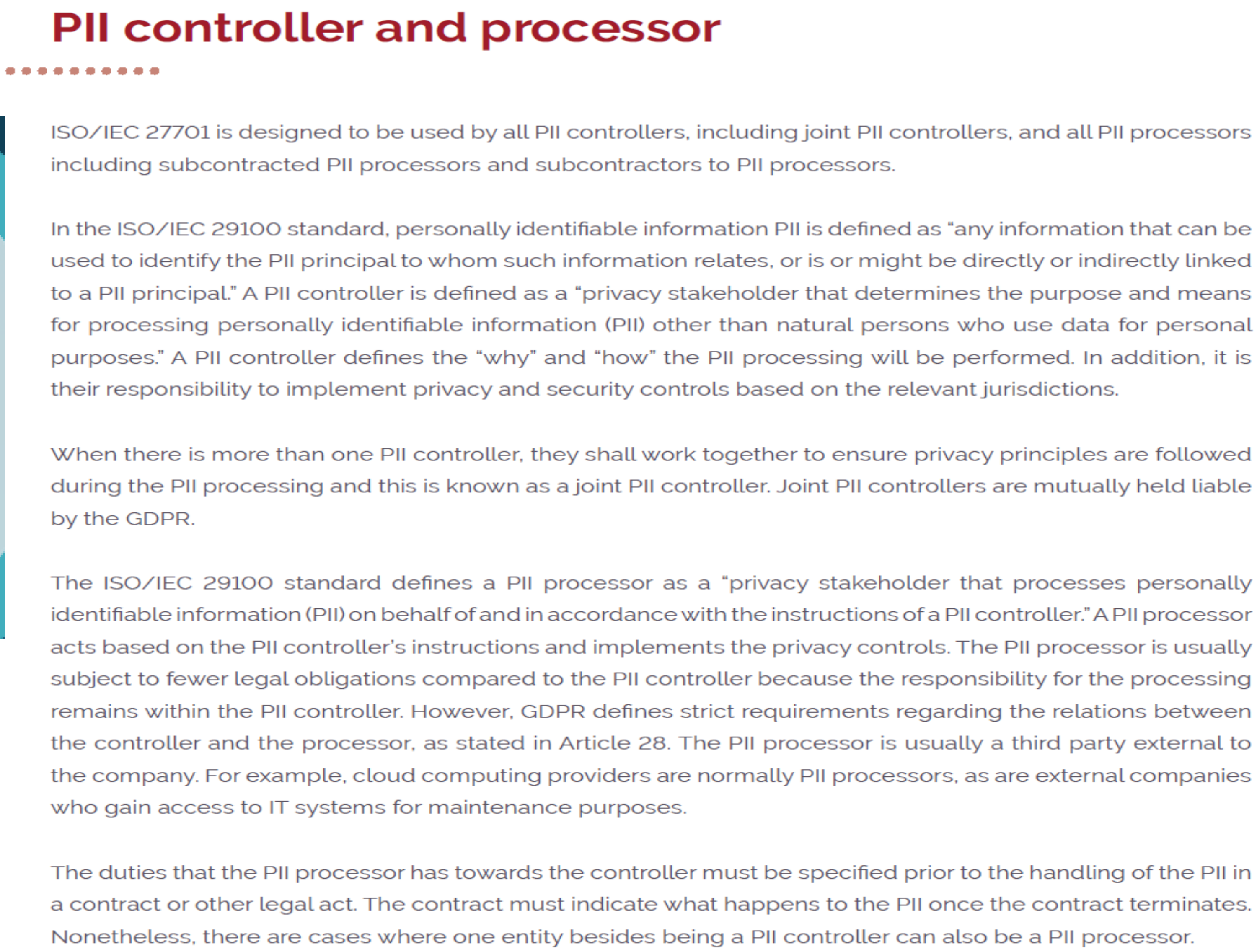
https://pecb.com/en/education-and-certification-for-individuals/iso-iec-27701/



PII Processor

.. privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller."

ISO/IEC 29100:2011



PII controller and processor

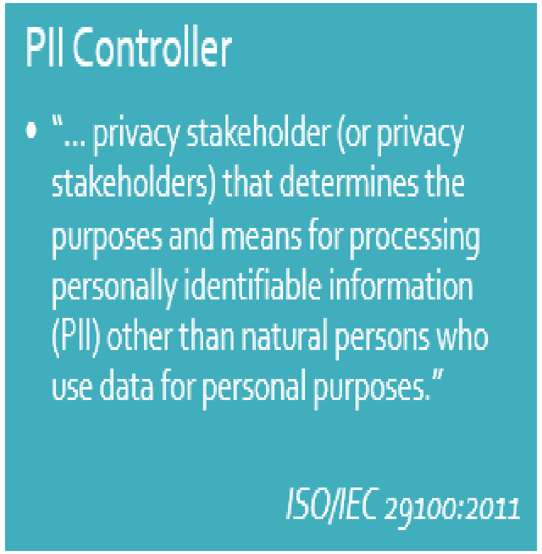
ISO/IEC 27701 is designed to be used by all PII controllers, including joint PII controllers, and all PII processors including subcontracted PII processors and subcontractors to PII processors.

In the ISO/IEC 29100 standard, personally identifiable information PII is defined as "any information that can be used to identify the PII principal to whom such information relates, or is or might be directly or indirectly linked to a PII principal." A PII controller is defined as a "privacy stakeholder that determines the purpose and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes." A PII controller defines the "why" and "how" the PII processing will be performed. In addition, it is their responsibility to implement privacy and security controls based on the relevant jurisdictions.

When there is more than one PII controller, they shall work together to ensure privacy principles are followed during the PII processing and this is known as a joint PII controller. Joint PII controllers are mutually held liable by the GDPR.

The ISO/IEC 29100 standard defines a PII processor as a "privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller." A PII processor acts based on the PII controller's instructions and implements the privacy controls. The PII processor is usually subject to fewer legal obligations compared to the PII controller because the responsibility for the processing remains within the PII controller. However, GDPR defines strict requirements regarding the relations between the controller and the processor, as stated in Article 28. The PII processor is usually a third party external to the company. For example, cloud computing providers are normally PII processors, as are external companies who gain access to IT systems for maintenance purposes.

The duties that the PII processor has towards the controller must be specified prior to the handling of the PII in a contract or other legal act. The contract must indicate what happens to the PII once the contract terminates. Nonetheless, there are cases where one entity besides being a PII controller can also be a PII processor.



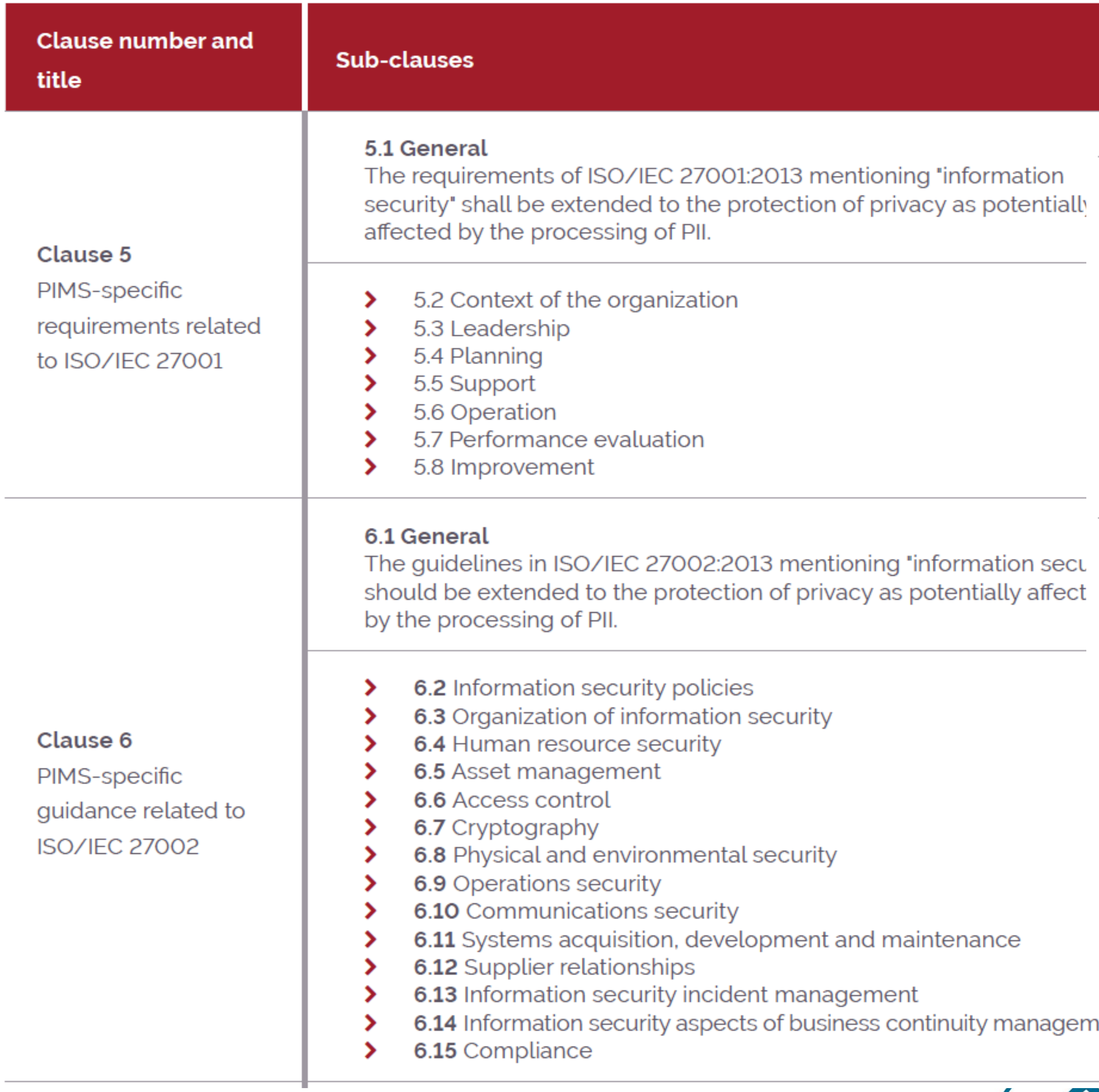
PII Controller

- "... privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes."

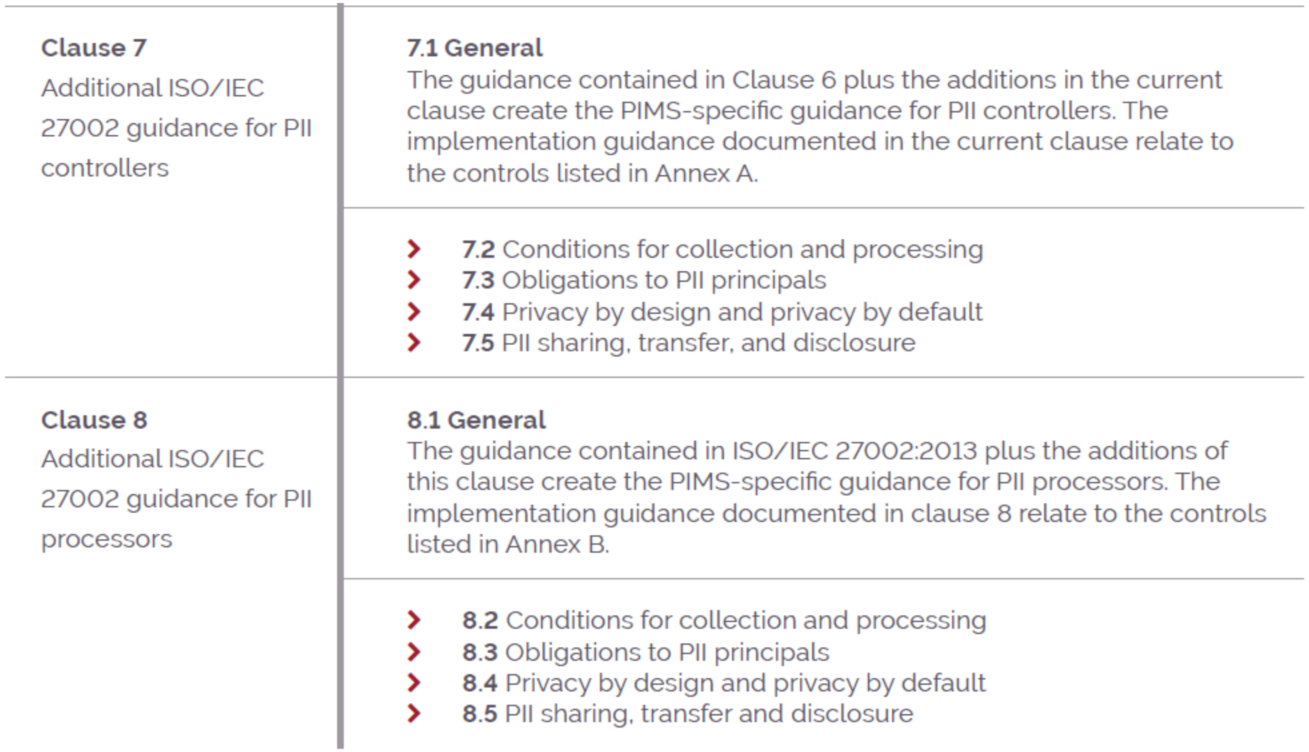
ISO/IEC 29100:2011

ISO 27701 - Privacy Information Management System (PIMS)

https://pecb.com/en/education-and-certification-for-individuals/iso-iec-27701/



Clause number and title	Sub-clauses
Clause 5 PIMS-specific requirements related to ISO/IEC 27001	**5.1 General** The requirements of ISO/IEC 27001:2013 mentioning "information security" shall be extended to the protection of privacy as potentiall affected by the processing of PII.
	› 5.2 Context of the organization › 5.3 Leadership › 5.4 Planning › 5.5 Support › 5.6 Operation › 5.7 Performance evaluation › 5.8 Improvement
Clause 6 PIMS-specific guidance related to ISO/IEC 27002	**6.1 General** The guidelines in ISO/IEC 27002:2013 mentioning "information secu should be extended to the protection of privacy as potentially affect by the processing of PII.
	› **6.2** Information security policies › **6.3** Organization of information security › **6.4** Human resource security › **6.5** Asset management › **6.6** Access control › **6.7** Cryptography › **6.8** Physical and environmental security › **6.9** Operations security › **6.10** Communications security › **6.11** Systems acquisition, development and maintenance › **6.12** Supplier relationships › **6.13** Information security incident management › **6.14** Information security aspects of business continuity management › **6.15** Compliance



Clause 7 Additional ISO/IEC 27002 guidance for PII controllers	**7.1 General** The guidance contained in Clause 6 plus the additions in the current clause create the PIMS-specific guidance for PII controllers. The implementation guidance documented in the current clause relate to the controls listed in Annex A.
	› **7.2** Conditions for collection and processing › **7.3** Obligations to PII principals › **7.4** Privacy by design and privacy by default › **7.5** PII sharing, transfer, and disclosure
Clause 8 Additional ISO/IEC 27002 guidance for PII processors	**8.1 General** The guidance contained in ISO/IEC 27002:2013 plus the additions of this clause create the PIMS-specific guidance for PII processors. The implementation guidance documented in clause 8 relate to the controls listed in Annex B.
	› **8.2** Conditions for collection and processing › **8.3** Obligations to PII principals › **8.4** Privacy by design and privacy by default › **8.5** PII sharing, transfer and disclosure

ISO 27701 - Privacy Information Management System (PIMS)

https://pecb.com/en/education-and-certification-for-individuals/iso-iec-27701/

Annex B – PIMS-specific reference control objectives and controls (PII Processors)
B.8.2 Conditions for collection and processing
B.8.8.2.1 Customer agreement
B.8.8.2.2.Organization's purposes
B.8.2.4 Infringing instruction
B.8.2.5 Customer obligations
8.8.2.6 Records related to processing PII
B.8.3 Obligations to PII principals
B.8.3..1 Obligations to PII Principals
B.8.4 Privacy by design and by default
B.8.4.1 Customer agreement
B.8.4.2.Organization's purposes
B.8.4.3 Infringing instruction
B.8.5 PII sharing, transfer and disclosure
8.5 PII sharing, transfer and disclosure
8.5.1 Basis for PII transfer between jurisdictions
8.5.2 Countries and international organizations to which PII can be transferred
8.5.3 Records of PII disclosure to third parties
8.5.4 Notification of PII disclosure requests
8.5.5 Legally binding PII disclosures
8.5.6 Disclosure of subcontractors used to process PII
8.5.7 Engagement of a subcontractor to process PII
8.5.8 Change of subcontractor to process PII

Table of Contents

- What are the Privacy Risks in the Age of Cloud Computing?
- Top Privacy Threats in the Cloud
- ISO Standards for Cloud Security and Privacy
- Tools and Techniques for PIMS Audits (ISO 27701)
- References + Q&A

CASE Study – Microsoft Supplier Security and Privacy Assurance Program (SSPA). **ISO 27701 Internal Audit – tools and methods** - 27701 | A-LIGN

- Leverage ISO 27001 + ISO 27701 to Meet Your Microsoft SSPA Requirements

- Microsoft requires that all vendors meet the requirements within the Supplier Security and Privacy Assurance Program (SSPA). This program requires that any vendor that collects, stores, or processes customer, partner, or employee information meet the reporting requirements. https://www.a-lign.com/service/microsoft-sspa.

- A Company operates securely under all Microsoft Data Protection Requirements providing high end support using Microsoft provided cloud-based services and tools. The sole use of cloud-based tooling allows our team to work efficiently with end customers while maintaining a low security risk, housing no customer or user data on any Company systems. Due to the nature of its business, Company assumes the role of, a Processor, as Company might access customer PII. Company has access to customer data, and potentially PII, but does not download, store or keep any PII or any other customer data in any direct managed system. However, the protection of customer privacy data a crucial business requirement as it's vital to Company to protect its reputation as well as the integrity and confidentiality of the services it provides to customers.

CASE Study – Microsoft Supplier Security and Privacy Assurance Program (SSPA).
ISO 27701 Internal Audit – Criteria and Schedule

Audit Criteria:v

- Review of the Implementation and effectiveness of ISMS and PIMS governance.
- The audit criteria (set of requirements) for this audit are all normative clauses of ISO/IEC 27001:2013 and ISO/IEC 27701-2019.
- Clause 4 – Context of the organization
- Clause 5 – Leadership/PIMS-specific requirements related to ISO/IEC 27001
- Clause 6 – Planning/PIMS-specific guidance related to ISO/IEC 27002
- Clause 7 – Support/Additional ISO/IEC 27002 guidance for PII controllers
- Clause 8 – Operation/Operation of the service management system/Additional ISO/IEC 27002 guidance for PII processors
- Clause 9 – Performance Evaluation
- Clause 10 – Improvement
- Annex A – Control objectives and controls/PIMS-specific reference control objectives and controls (PII Controllers)
- Annex B – PIMS-specific reference control objectives and controls (PII Processors)

9am	Clause 5. PIMS-specific requirements related to ISO/IEC 27001
	5.1 General
	5.2 Context of the organization
	5.4 Planning
10am	Annex A - PIMS-specific reference control objectives and controls (PII Controllers)
	.7.2 Conditions for collection and processing
	A.7.3 Obligations to PII principals
	A.7.4 Privacy by design and privacy by default
	A.7.5 PII sharing, transfer and disclosure
11am	Annex B – PIMS-specific reference control objectives and controls (PII Processors)
	B.8.2 Conditions for collection and processing
	B.8.3 Obligations to PII principals
	B.8.4 Privacy by design and by default
	B.8.5 PII sharing, transfer and disclosure

CASE Study – ISO 27701 Internal Audit – Documentation Review

	Document Name
1	Context of the Organization (scope & boundaries)
2	Information Security Policy
3	Roles, Responsibilities and Authorities
4	Organization Chart (Roles, Responsibilities)
7	Privacy Risk Assessment
8	Risk Treatment Plan
9	Statement of Applicability
10	Data Privacy Policy
17	Information Classification and Handling Policy
18	Privacy Impact Assessment

CASE Study – ISO 27701 Internal Audit – Audit Conclusions

In the Opinion of the Auditor, the organization currently conforms to the ISO 27001 Clause 4-10 / Annex A generic requirements for an Information Security Management System (ISMS).

In the Opinion of the Auditor, the organization currently conforms to the ISO 27701 applicable clauses 5 and 6 / Annex B guidance for PII Processor (PIMS).

The areas assessed during the course of the visit were found to be very effective, very well controlled and managed. Company shows continual improvement in managing the ISMS program by communicating core principles of privacy and information security (protection of confidentiality, integrity and availability) across the organization.

Non-conformities

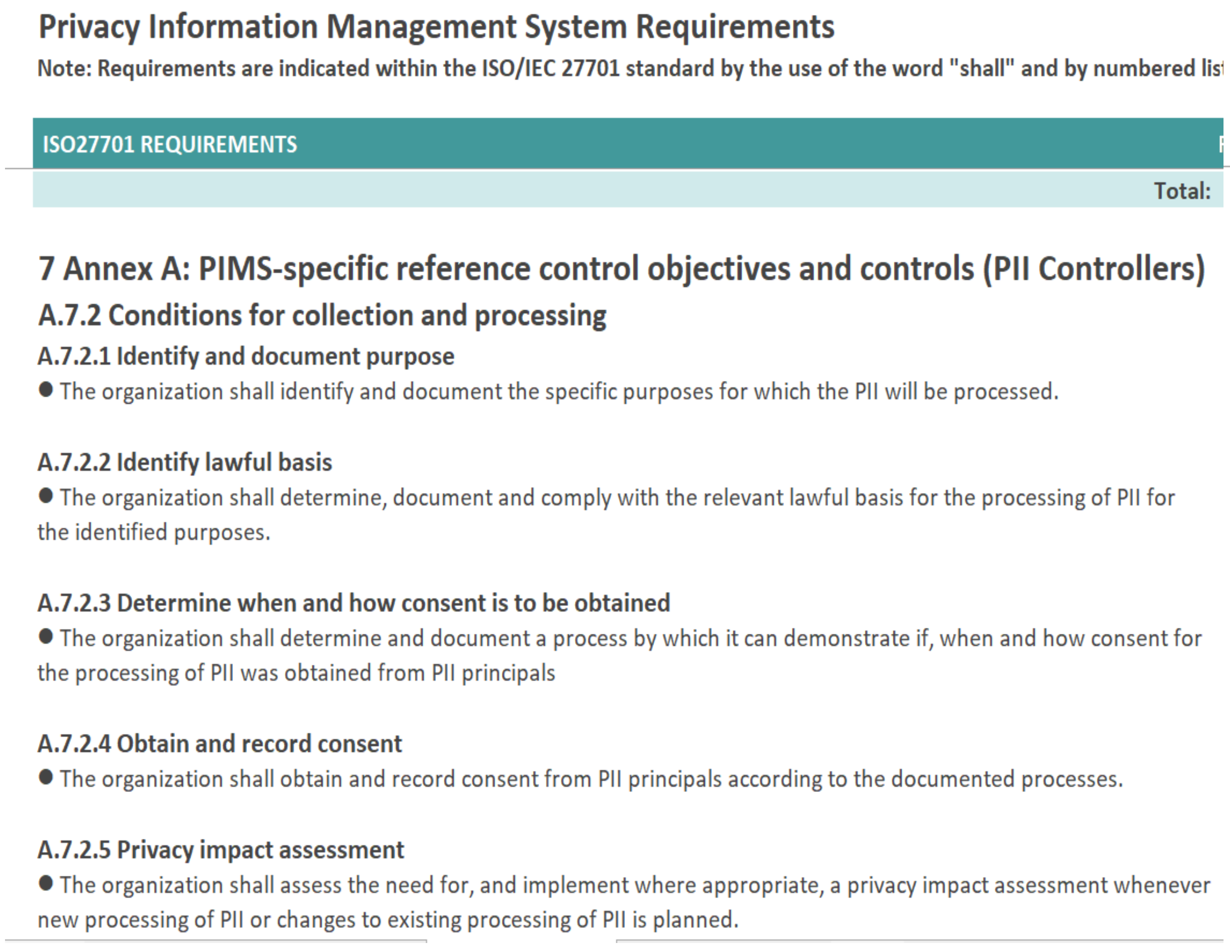
No major non-conformities have been identified in the ISMS/PIMS Internal Audit

Minor NCR

Minor Non-Conformity - 01 5.4.1.2 (ISO 27701) - PIMS risk assessment does not include the applicable ISO 27701 Annex B requirements for a Data Processor (B.8.x)

Minor Non-Conformity - 02 A.12.4.2 Logs must be safeguarded from tampering.

Summary PIMS Requirements for PII Controllers and Principals



Privacy Information Management System Requirements

Note: Requirements are indicated within the ISO/IEC 27701 standard by the use of the word "shall" and by numbered lis

ISO27701 REQUIREMENTS

Total:

7 Annex A: PIMS-specific reference control objectives and controls (PII Controllers)

A.7.2 Conditions for collection and processing

A.7.2.1 Identify and document purpose

- The organization shall identify and document the specific purposes for which the PII will be processed.

A.7.2.2 Identify lawful basis

- The organization shall determine, document and comply with the relevant lawful basis for the processing of PII for the identified purposes.

A.7.2.3 Determine when and how consent is to be obtained

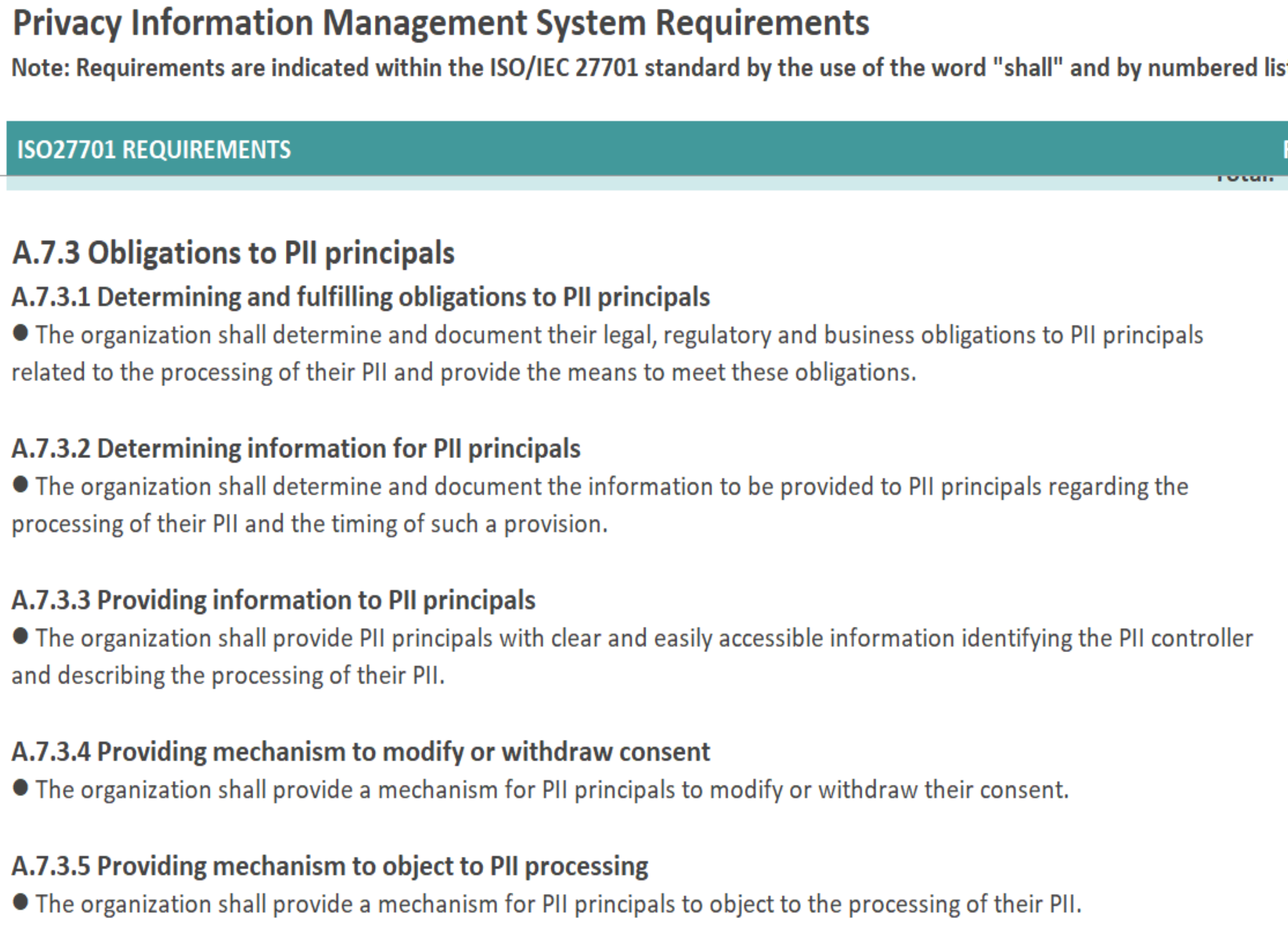
- The organization shall determine and document a process by which it can demonstrate if, when and how consent for the processing of PII was obtained from PII principals

A.7.2.4 Obtain and record consent

- The organization shall obtain and record consent from PII principals according to the documented processes.

A.7.2.5 Privacy impact assessment

- The organization shall assess the need for, and implement where appropriate, a privacy impact assessment whenever new processing of PII or changes to existing processing of PII is planned.



Privacy Information Management System Requirements

Note: Requirements are indicated within the ISO/IEC 27701 standard by the use of the word "shall" and by numbered lis

ISO27701 REQUIREMENTS

A.7.3 Obligations to PII principals

A.7.3.1 Determining and fulfilling obligations to PII principals

- The organization shall determine and document their legal, regulatory and business obligations to PII principals related to the processing of their PII and provide the means to meet these obligations.

A.7.3.2 Determining information for PII principals

- The organization shall determine and document the information to be provided to PII principals regarding the processing of their PII and the timing of such a provision.

A.7.3.3 Providing information to PII principals

- The organization shall provide PII principals with clear and easily accessible information identifying the PII controller and describing the processing of their PII.

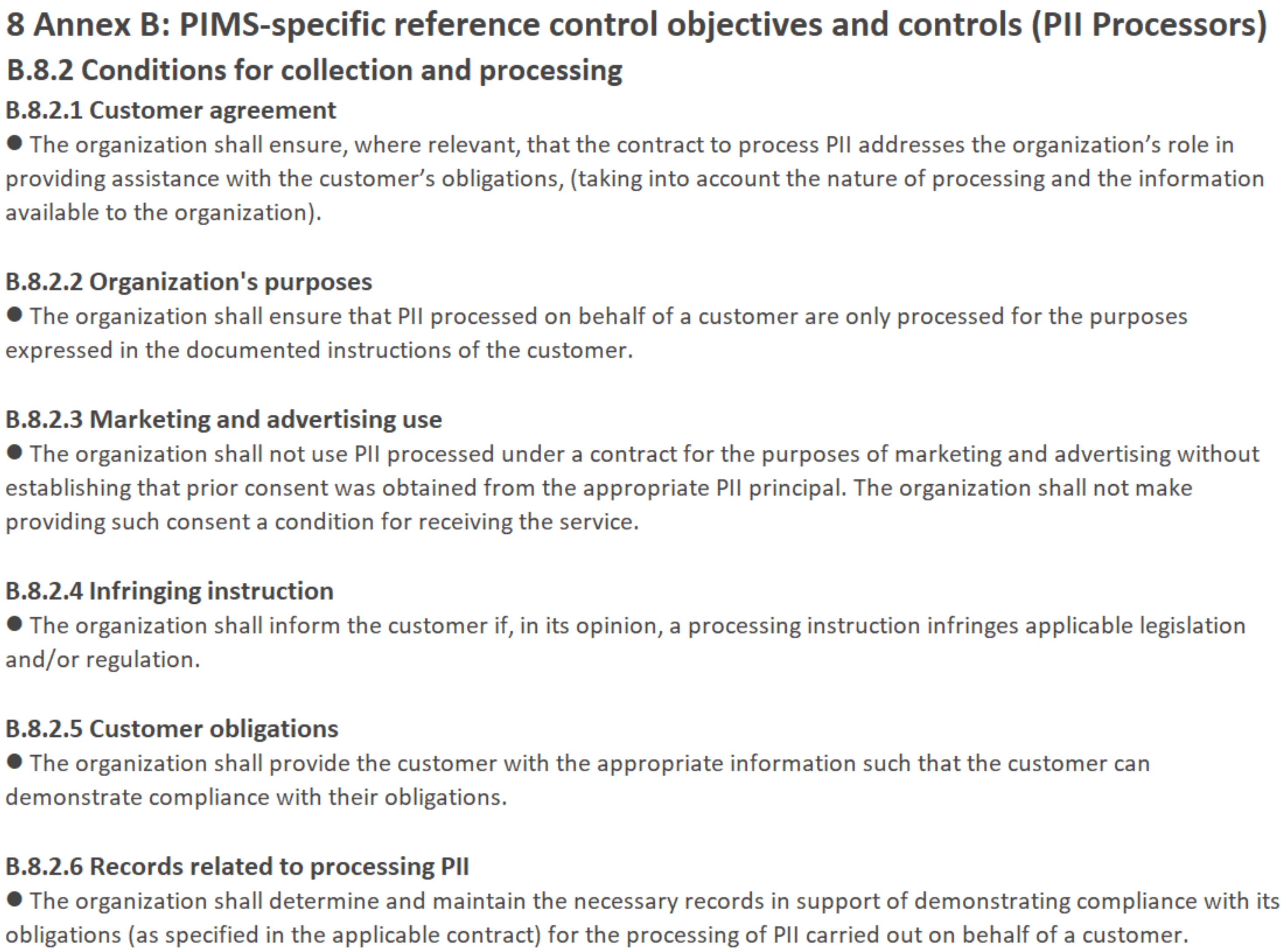
A.7.3.4 Providing mechanism to modify or withdraw consent

- The organization shall provide a mechanism for PII principals to modify or withdraw their consent.

A.7.3.5 Providing mechanism to object to PII processing

- The organization shall provide a mechanism for PII principals to object to the processing of their PII.

Summary PIMS Requirements for PII Controllers and Processors



8 Annex B: PIMS-specific reference control objectives and controls (PII Processors)

B.8.2 Conditions for collection and processing

B.8.2.1 Customer agreement

- The organization shall ensure, where relevant, that the contract to process PII addresses the organization's role in providing assistance with the customer's obligations, (taking into account the nature of processing and the information available to the organization).

B.8.2.2 Organization's purposes

- The organization shall ensure that PII processed on behalf of a customer are only processed for the purposes expressed in the documented instructions of the customer.

B.8.2.3 Marketing and advertising use

- The organization shall not use PII processed under a contract for the purposes of marketing and advertising without establishing that prior consent was obtained from the appropriate PII principal. The organization shall not make providing such consent a condition for receiving the service.

B.8.2.4 Infringing instruction

- The organization shall inform the customer if, in its opinion, a processing instruction infringes applicable legislation and/or regulation.

B.8.2.5 Customer obligations

- The organization shall provide the customer with the appropriate information such that the customer can demonstrate compliance with their obligations.

B.8.2.6 Records related to processing PII

- The organization shall determine and maintain the necessary records in support of demonstrating compliance with its obligations (as specified in the applicable contract) for the processing of PII carried out on behalf of a customer.

Table of Contents

- What are the Privacy Risks in the Age of Cloud Computing?
- Top Privacy Threats in the Cloud
- ISO Standards for Cloud Security and Privacy
- Tools and Techniques for PIMS Audits (ISO 27701)
- References + Q&A

ISO 27001/27701 Accredited Site List (examples)

Google - https://cloud.google.com/security/compliance/iso-27701

AWS - https://aws.amazon.com/blogs/security/aws-achieves-iso-iec-27701-2019-certification/

https://aws.amazon.com/compliance/iso-certified/

OneTrust (Coalfire) - https://www.onetrust.com/news/onetrust-achieves-worlds-first-iso-27701/

Xi Cloud Services (Nutanix) Achieve ISO/IEC 27701:2019 Certification

https://next.nutanix.com/community-blog-154/xi-cloud-services-achieve-iso-iec-27701-2019-certification-38471

Microsoft PIMS - https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27701

CubePay - Singapore TuV SuD (Fintech)

https://www.tuvsud.com/en-us/services/auditing-and-system-certification/iso-27701

dacadoo Obtains ISO 27001 and ISO 27701 Certifications – https://dacadoo.pr.co/199390-dacadoo-obtains-iso-27001-and-iso-27701-certifications

Teleperformance (France)

https://www.teleperformance.com/en-us/insights-list/insightful-articles/global/elevating-data-privacy-around-the-world-with-global-iso-27701-certification/

https://www.businesswire.com/news/home/20211201005742/en/Teleperformance-A

IEEE Digital Privacy Initiative

- An IEEE-wide effort focusing on the digital privacy needs of individuals, rather than the security of data/products/organization
  - Envision a future in which the capability exists to enable any individual around the world to privately maintain presence, data, identity, and dignity online
- To help achieve this vision, the Initiative seeks the following goals:
  - Bring the ***voice of technologists*** to the digital privacy conversation, incorporating a holistic approach to address privacy that also includes economic, legal, and social perspectives
  - Facilitate cross-disciplinary collaboration to advance research, promote standardization and best practices, and create tools and capabilities to support the privacy needs of individuals, and
  - Coordinate efforts across and beyond IEEE with a multicultural lens that are working on different dimensionns of digital privacy
  - ***Feel free to contact/connect with us @ digitalprivacyinfo@ieee.org***

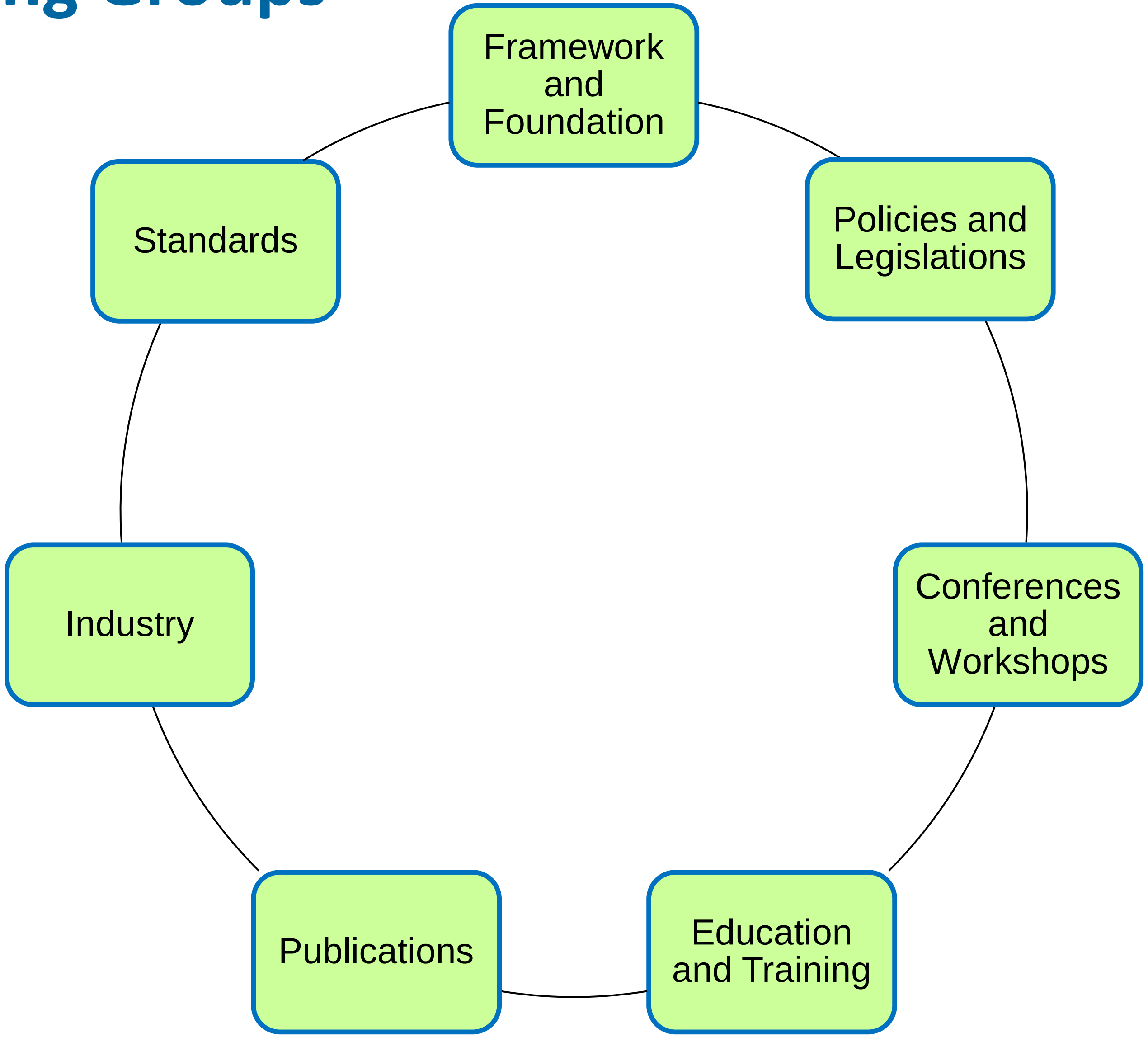
Learn more at digitalprivacy.ieee.org

Digital Privacy Initiative Working Groups

Healthcare

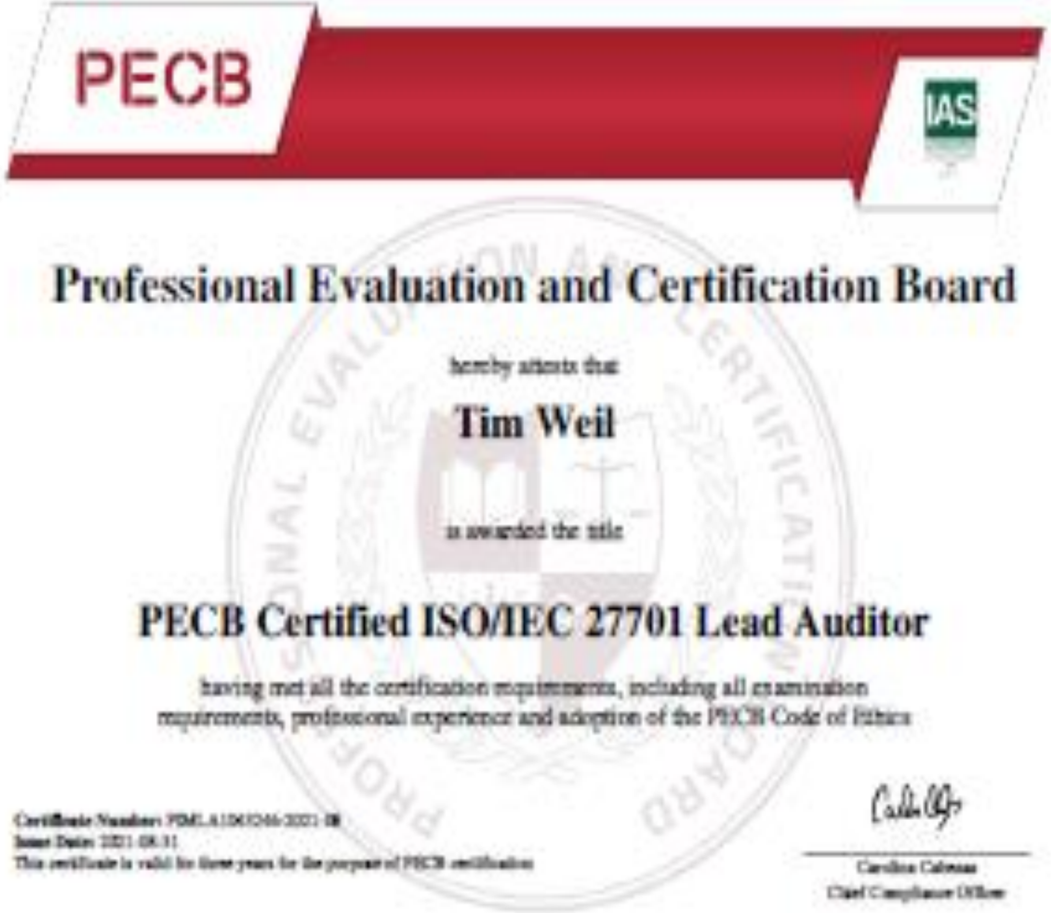
Connected Vehicles

Energy



Assessing Privacy Information Management Requirements – Blue Sky or Rain?

Audit and Trainer – ISO 27701 (Privacy Information Management)



PECB

IAS

Professional Evaluation and Certification Board

hereby attests that

Tim Weil

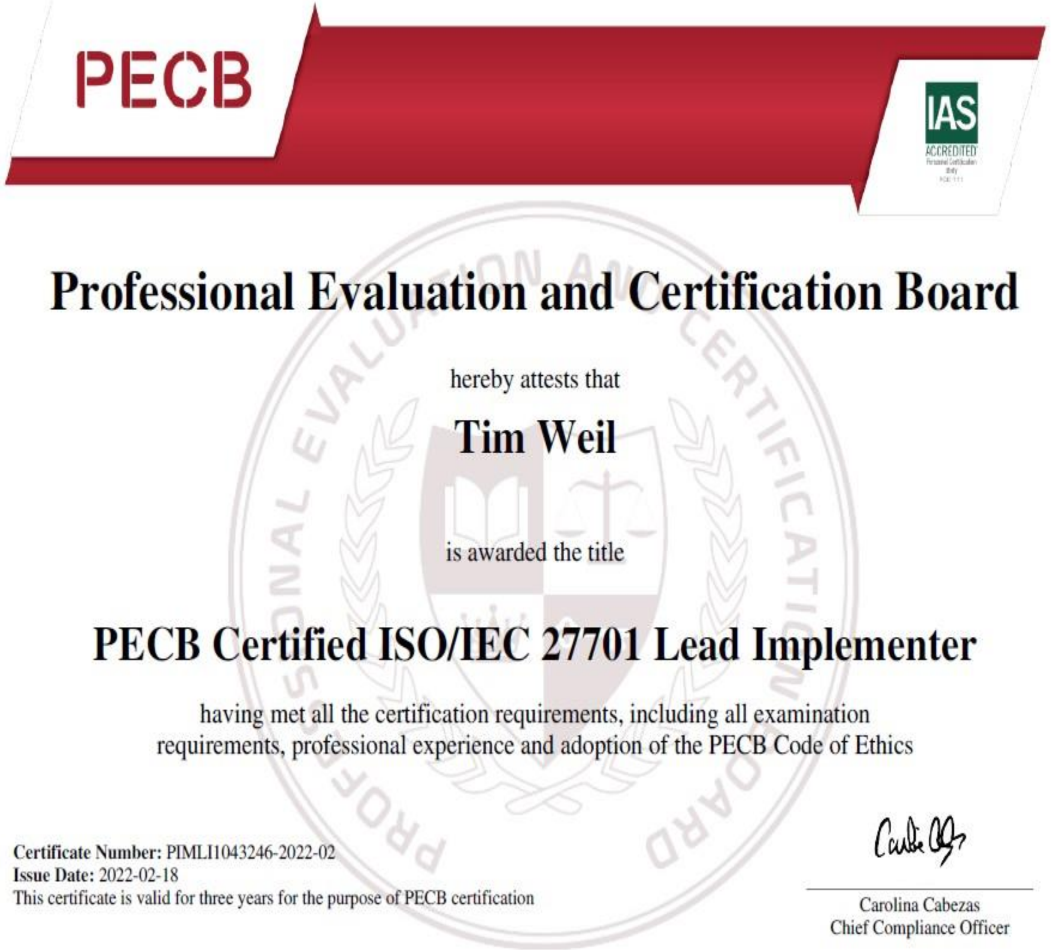
is awarded the title

PECB Certified ISO/IEC 27701 Lead Auditor

having met all the certification requirements, including all examination requirements, professional experience and adoption of the PECB Code of Ethics

Certificate Number: PIMLA1043246-2021-08
Issue Date: 2021-08-31
This certificate is valid for three years for the purpose of PECB certification

Carolina Cabezas
Chief Compliance Officer



PECB

IAS
ACCREDITED

Professional Evaluation and Certification Board

hereby attests that

Tim Weil

is awarded the title

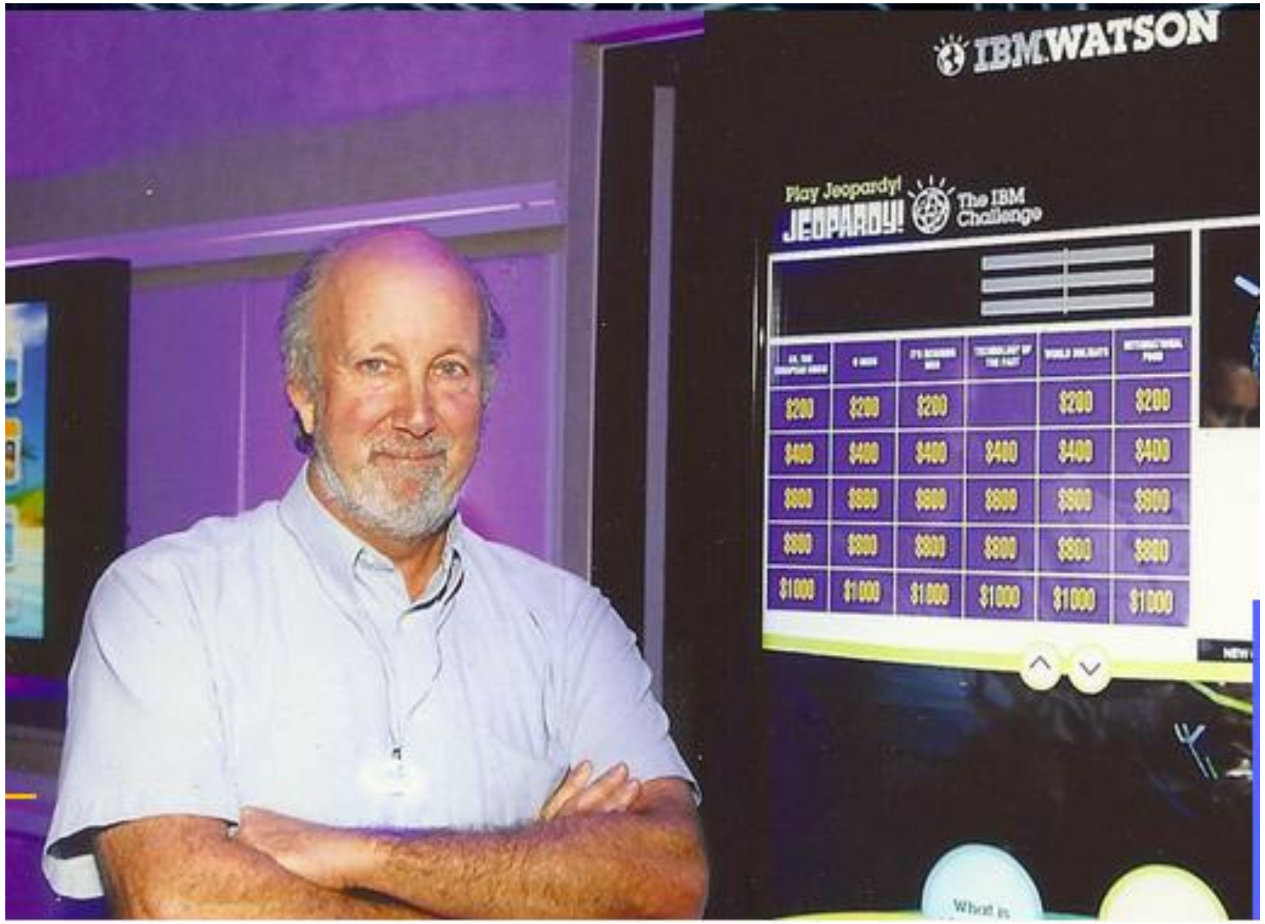
PECB Certified ISO/IEC 27701 Lead Implementer

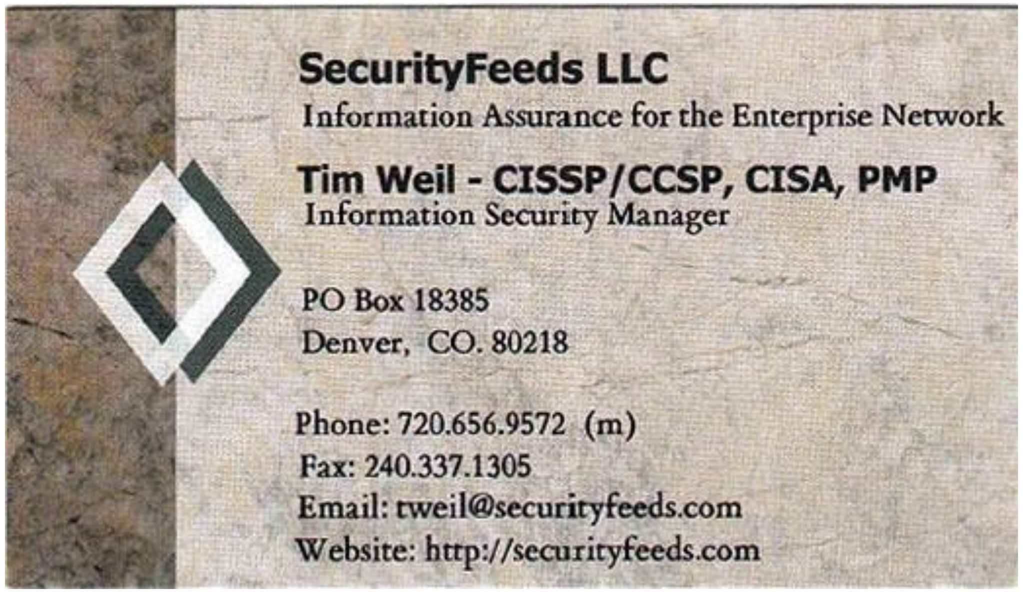
having met all the certification requirements, including all examination requirements, professional experience and adoption of the PECB Code of Ethics

Certificate Number: PIMLI1043246-2022-02
Issue Date: 2022-02-18
This certificate is valid for three years for the purpose of PECB certification

Carolina Cabezas
Chief Compliance Officer

Thank you for joining us!





SecurityFeeds LLC
Information Assurance for the Enterprise Network

Tim Weil - CISSP/CCSP, CISA, PMP
Information Security Manager

PO Box 18385
Denver, CO. 80218

Phone: 720.656.9572 (m)
Fax: 240.337.1305
Email: tweil@securityfeeds.com
Website: http://securityfeeds.com

SecurityFeeds LLC provides IT Management Consulting services

- Communications and Security Engineering
- Data Processing (Systems Engineering)
- Project and Program Management
- Risk Management (ISO 27001)

Our expertise includes Enterprise Security Architecture, Cloud Security, Program Management, and Network Engineering.

"RISK is a four-letter word"

http://www.securityfeeds.com - trweil@ieee.org