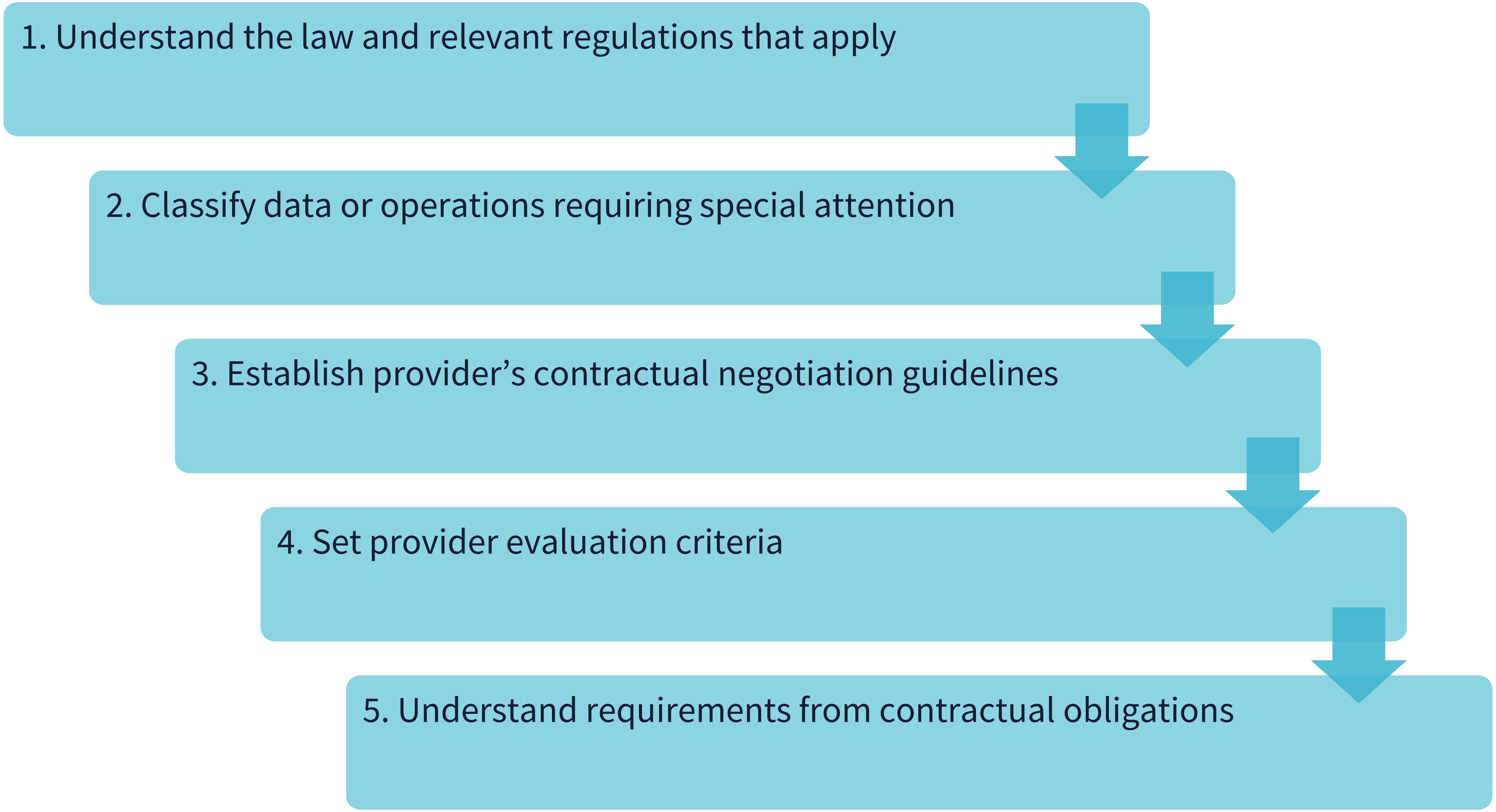
Conflicting International Legislation

- Customers of cloud service providers must be cognizant of the regions in which data is stored and content is distributed
- Cloud providers must remember that they may still be subject to mandates in conducting business with certain jurisdictions – even if the organization does not reside there

Evaluation of Legal Risks in Cloud Computing

- Data privacy and security: GDPR, PCI-DSS, HIPAA
- Data ownership: intellectual property rights and DRM/IRM in various agreements and contracts
- Liability for copyright infringement, data breaches, and privacy violations
- Primary and secondary loss
- Legal issues resulting from counter-attack active defense
- Jurisdictional issues: import-export, cultural sensitivities

Setting Legal and Regulatory Requirements



1. Understand the law and relevant regulations that apply

2. Classify data or operations requiring special attention

3. Establish provider’s contractual negotiation guidelines

4. Set provider evaluation criteria

5. Understand requirements from contractual obligations

ISO/IEC 27050

- Information Technology Electronic Discovery Package offers guidance methods on establishing the electronic discovery process
- The ISO/IEC 27050 series enables the user to identify, collect, preserve, process, review, and analyze electronically-stored information

ISO/IEC 27050

- Electronic discovery often serves as a driver for investigations as well as evidence acquisition and handling activities
- Exam: it is not intended to contradict or supersede local jurisdictional laws and regulations

The eDiscovery Process

1. **Identification**: electronically stored information (ESI) that is possibly significant to a case is recognized, along with its locations, custodians, sizes/volumes, etc.

2. **Preservation**: the identified, potentially relevant ESI is placed under a legal hold, starting the official forensic process designed to ensure, beyond doubt, that the info is protected

3. **Collection**: ESI is assembled from the original custodian, usually by physically removing the original digital storage media into a safe chain of custody

The eDiscovery Process

4. **Processing**: forensic bit copies are stored in a manner that lets them be searched or analyzed for information and knowledge that is applicable to the case, using appropriate forensic tools and platforms

5. **Review**: forensic bit copies are searched or analyzed for information that is relevant to the case

6. **Analysis**: the information is further scrutinized and evaluated as to its significance, suitability, weight, connotation, implications, etc.

7. **Production**: applicable information from the analysis, plus the original storage media, etc., is officially offered to the court as evidence

Issues with PHI and PII in the Cloud

- When exposing data to customers on public virtual servers or with content delivery networking, cloud consumers must be cognizant of jurisdictional laws, regulation, and cultural/religious sensitivities
- Cloud-based tokenization engines are popular solutions for anonymizing personal identifiable and health information from datasets

Issues with PHI and PII in the Cloud

- In cloud computing, the legal responsibility for data processing falls to the consumer or user who solicits the services of a CSP
- As in all other cases in which a third party is given the task of processing personal data, the user, or data controller, is responsible for ensuring that the relevant requirements for the protection and compliance with requirements for **personally identifiable information (PII)** and **protected health information (PHI)** are met

Contractual PII

- Where an organization or entity processes, transmits, or stores PII as part of its business or services, this information is required to be adequately protected in line with relevant local state, national, regional, federal, or other laws
- The relevant contract should list the applicable rules and requirements from the organization that "owns" the data and the laws that apply to the provider

Regulated PII

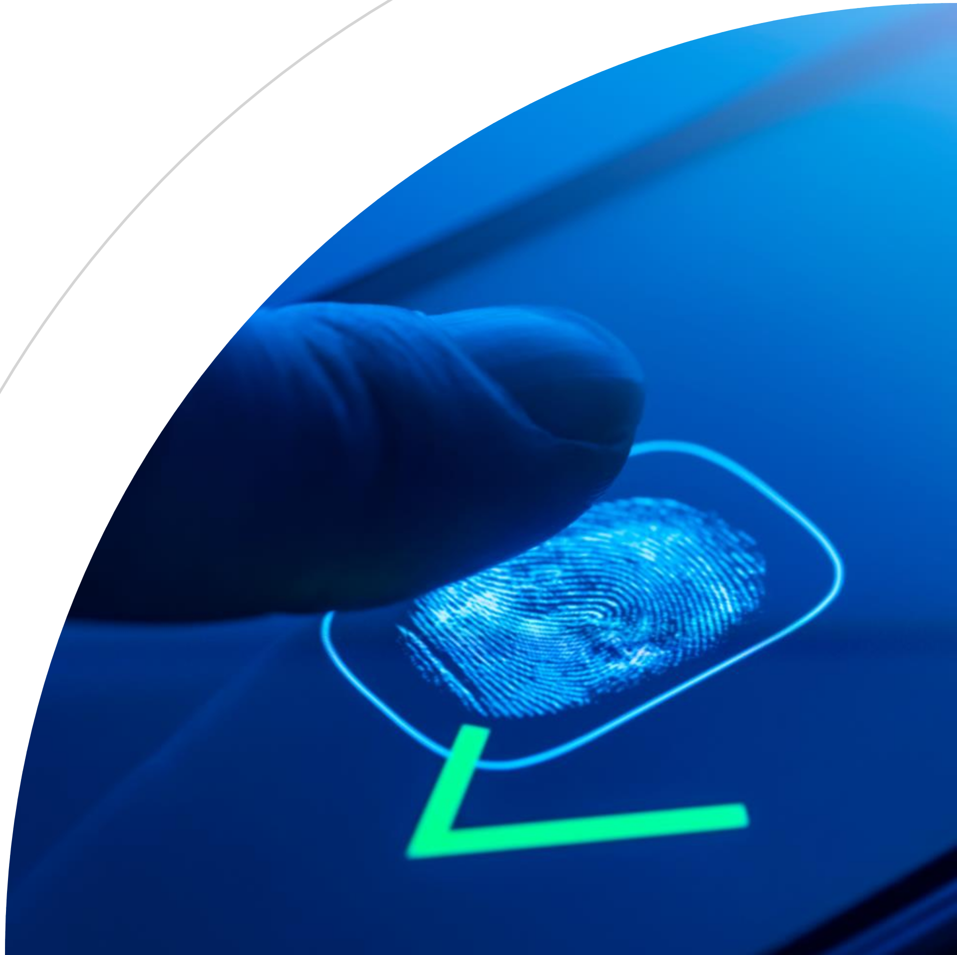
The key focus and distinct criteria to which the regulated PII must adhere is required under law and statutory requirements, as opposed to the contractual criteria that may be based on best practice or organizational security policies

ISO/IEC 27002

- Establishes commonly-accepted control objectives and best practices for implementing measures to protect PII in line with the privacy principles in ISO/IEC 29100 for the public cloud computing environment
- Stipulates guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of PII which can apply to a public cloud service provider's information security risk environment

ISO/IEC 27002

- ISO/IEC 27002 applies to all types and sizes of organizations, including public and private companies, government entities, and not-for-profit organizations, which provide information processing services as PII processors using contractual cloud computing with other entities
- The guidelines can also apply to enterprises acting as PII controllers
- However, PII controllers can be subject to additional PII protection legislation, regulations and obligations, not applying to PII processors



GAPP and PMF

- The **Privacy Management Framework (PMF)** is often used as an initial component in launching and operating a comprehensive information privacy initiative
- The program will address privacy responsibilities and risks while enabling current and future business opportunities
- The PMF was created as an update to the former 2009 **Generally Accepted Privacy Principles (GAPP)**
- Because of significant changes in technologies and in global, country-specific, local information and data privacy laws and standards, including the publication of the GDPR, the AICPA Privacy Task Force updated the PMF in 2020

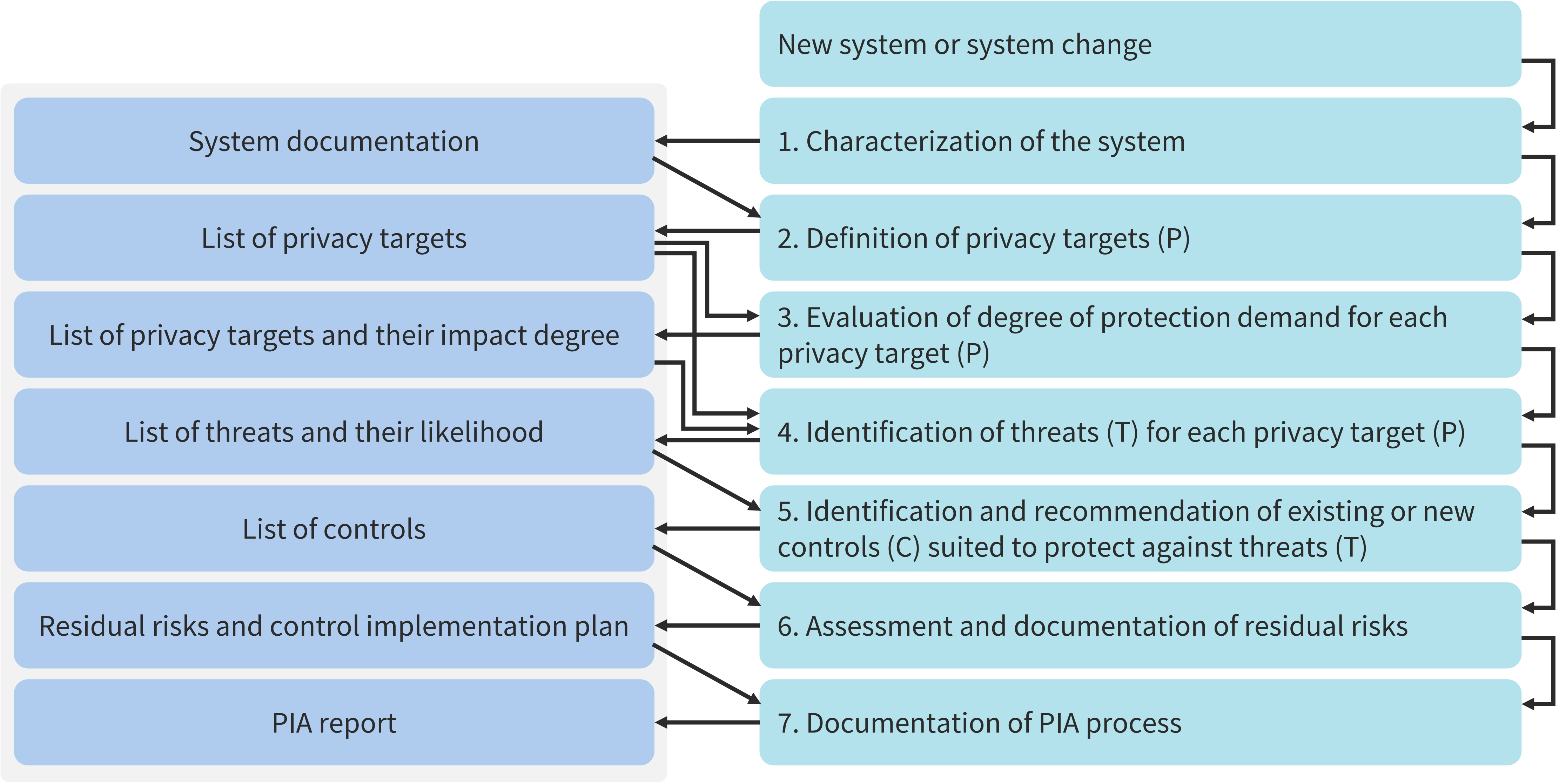
Privacy Impact Assessment

- A privacy impact assessment (PIA) is an analysis of how personally identifiable information (PII) is treated to maintain compliance with applicable regulations
- It governs the risks associated with information systems or activities, and finds ways to reduce the risks to privacy

Privacy Impact Assessment

- The PIA is a decision tool used by DHS to identify and mitigate privacy risks and notify the public on
  - What PII DHS is collecting
  - Why the PII is being collected
  - How the PII will be collected, used, accessed, shared, safeguarded, and stored

Privacy Impact Assessment: Process



New system or system change

1. Characterization of the system

2. Definition of privacy targets (P)

3. Evaluation of degree of protection demand for each privacy target (P)

4. Identification of threats (T) for each privacy target (P)

5. Identification and recommendation of existing or new controls (C) suited to protect against threats (T)

6. Assessment and documentation of residual risks

7. Documentation of PIA process

System documentation

List of privacy targets

List of privacy targets and their impact degree

List of threats and their likelihood

List of controls

Residual risks and control implementation plan

PIA report

Risk Treatment: Acceptance

- Risk treatment is also referred to as handling or appetite
- Do not implement any safeguards or controls to lessen residual risk
- The controls considered may not provide adequate return on investment
- The level of risk is deemed tolerable
- Justification in writing or in person is often required from a security engineer or architect

Risk Treatment: Avoidance

- Involves choosing not to undertake actions that introduce risk or raise vulnerability to an unacceptable level
- A cloud customer may decide not to put data in certain regions or even not upload the data at all
- May not use CloudHSM instead of locally placing it in an on-site data center
- Remember that being too risk averse can lead to lost opportunities and exposure to new enabling technologies

Risk Treatment: Transference

- Involves passing some or all risk to a third party
- This factor will drive decisions around cloud service types and shared responsibility models
  - Insurance company policies
  - Cloud service providers, MSSPs, and CASBs
  - Reciprocal agreements for disaster recovery sites

Risk Treatment: Mitigation

- Implement safeguards that will eliminate or reduce risk exposure
- Risk may exist, but the impact is reduced
- Administrative, physical, and technical control categories
- Preventative, detective, corrective, compensating, deterrent control types

NIST SP 800-30

NIST SP 800-30 Risk Management Guide for Information Technology Systems states:

- If control would reduce risk more than needed, then see whether a less expensive alternative exists
- If control would cost more than the risk reduction provided, then find something else
- If control does not reduce risk sufficiently, then look for more controls or a different control
- If control provides enough risk reduction and is cost-effective, then use it

CSA Cloud Controls Matrix

- The CSA Cloud Controls Matrix (CCM) includes 197 control objectives structured in 17 domains covering all key aspects of cloud technology
- Often used for the systematic assessment of a cloud implementation
- Offers guidance on which security controls should be implemented by which actor within the cloud supply chain
- CCM is considered the de facto standard for cloud security assurance and compliance

Consensus Assessment Initiative Questionnaire

STAR Level 1: Security Questionnaire (Consensus Assessment Initiative Questionnaire v4 / CAIQ v4) offers an industry-accepted way to document what security controls exist in IaaS, PaaS, and SaaS services

Metrics for Risk Management: CCM Domains

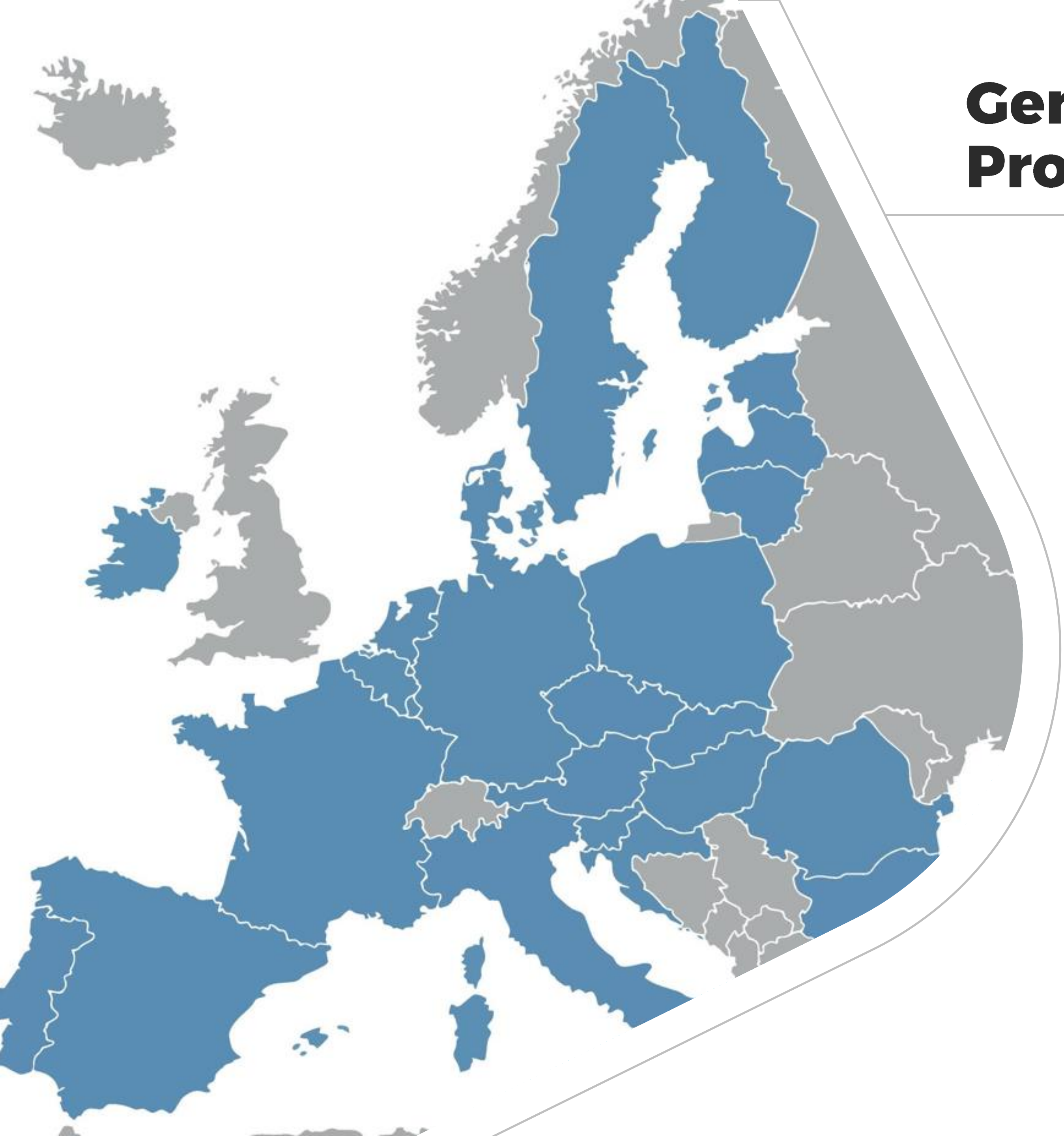
- Application and interface security (AIS)
- Audit assurance and compliance (AAC)
- Business continuity management and operational resilience (BCR)
- Change control and configuration management (CCC)
- Data security and information lifecycle management (DSI)
- Datacenter security (DCS)
- Encryption and key management (EKM)
- Governance and risk management (GRM)
- Human resources (HRS)
- Identity and access management (IAM)
- Infrastructure and virtualization security (IVS)
- Interoperability and portability (IPY)
- Mobile security (MOS)
- Security incident management, eDiscovery, and cloud forensics (SEF)
- Supply chain management, transparency, and accountability (STA)
- Threat and vulnerability management

The Sarbanes-Oxley Act

- CEOs and CFOs are obligated under the Sarbanes-Oxley Act (SOX) to ensure that financial records are precise, and that reports submitted to the SEC are accurate
- They are penalized for non-compliance even if the non-compliance was accidental
- SOX covers not only financial records and reporting – it also has compliance sections on data security and IT
- Companies must maintain records proving they comply with SOX, and then undergo an annual audit, the results of which must be easily available to all stakeholders
- SOX contains 11 sections

The Sarbanes-Oxley Act

- Companies that must comply with the Sarbanes-Oxley Act (SOX) include:
  - US publicly-traded companies larger than a certain size – it doesn’t matter where the stocks are traded: NYSE, Nasdaq, and over the counter stocks are all subject to SOX compliance
  - Foreign companies that have registered debt or equity with the US Security and Exchange Commission (SEC)
  - Accounting firms that audit companies required to comply with SOX must also comply with SOX



General Data Protection Regulation

- General Data Protection Regulation (GDPR) addresses data protection and privacy in the EU and all other areas, citizens, and areas under its jurisdiction, regardless of where the data is created, used, or stored
- It does apply to other countries doing business with EU entities and is very strict
- The European Court of Justice (ECJ) nullified the U.S.-EU Safe Harbor agreement between the EU and the U.S. Department of Commerce in 2015

General Data Protection Regulation

- The Privacy Shield Framework then replaced Safe Harbor
- March 25, 2022: The U.S. and European Commission announced an agreement in principle on a new "Trans-Atlantic Data Privacy Framework" to foster trans-Atlantic data flows and address concerns raised by the Court of Justice of the EU in the Schrems II decision of July 2020