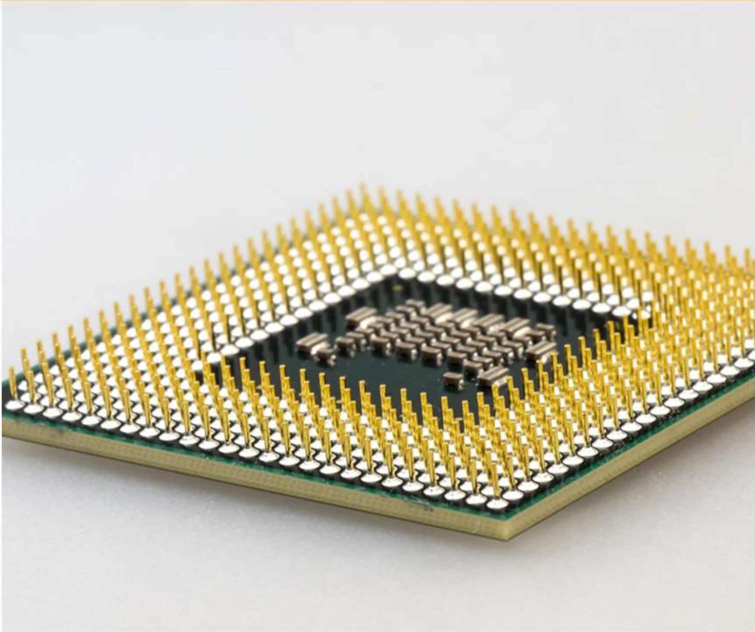
Trade Compliance – Technology Control Plan

SECO Exportkontrolltagung

Architecture for a Technology Control Plan
www.pwc.ch/en/services/tax-advice/customs.html



Agenda

1. Vorstellung PwC Team 03
2. Was bedeutet Trade Compliance 08
3. Der Technology Control Plan (TCP) (Fokus immaterielle Güter) 12

1

Vorstellung PwC Team

PwC Team – Trade Compliance – Technology Control Plan

Simeon Probst
Partner

Qualifications

- lic. iur. University of Basel
- Certified Swiss Tax Expert with federal diploma

Professional Experience

- Simeon joined PwC in 2000. He is leading the Customs and International Trade team in Basel and is the leader of the customs consulting of PwC Switzerland.
- With his extensive experience and background, Simeon participates as a speaker in PwC and external VAT and customs seminars and has teaching assignments at «EXPERTsuisse», the Swiss Fiduciary Chamber and the Swiss Accountancy Academy.
- He has published articles in professional journals and is co-author of the Swiss customs commentary (export and bonded warehouses

Relevant Experience

- Simeon’s biggest clients, Swiss quoted multinationals, have all introduced new centralized supply chain models in recent years, giving him detailed knowledge of VAT, customs planning opportunities, export controls and the pitfalls of such projects.
- Simeon has worked on a wide range of projects including VAT, customs and export control support
- Introduction of a new distribution model for a Swiss steel group using fully fledged manufacturers and agents (e.g. preferential origin), VAT and customs support for the implementation of a worldwide principal structure for a Swiss manufacturer of medical technology

Lorenz Neher
Senior Manager

Qualifications

Compliance Management, Diploma of Advanced Studies, Executive Master of Business Studies, Lucerne School of Business, Bachelor of Science , Electronic Engineering (Lucerne University of Applied Sciences and Arts), CISSP (ISC)^2, CISA, CRISC (ISACA), TOGAF ® 9 Certified

Professional Background

Lorenz has a proven track record of more than 20 years in supporting organizations to design, implement and run IT- and Security-Solution in order to protect data appropriately and achieve compliance, cybersecurity and resilience. He has vast experience in life science, healthcare, government, financial services, and telecommunication.

Relevant Experience and Projects (extract)

- Subject Matter Expert for compliance management for IT and technology. This includes:
  - IT Governance to identify, categorise and classify compliance relevant data
  - Derive from legal and regulatory requirements a control framework for organisational and technical controls in the IT
  - Technology enablement for access control and data protection
  - Compliance Monitoring
- Security Architecture reviews and implementation planning for mid size and large enterprises to ensure compliance to various legal and regulatory requirements

PwC Switzerland & Principality of Liechtenstein

as per April 2021

192 Partner

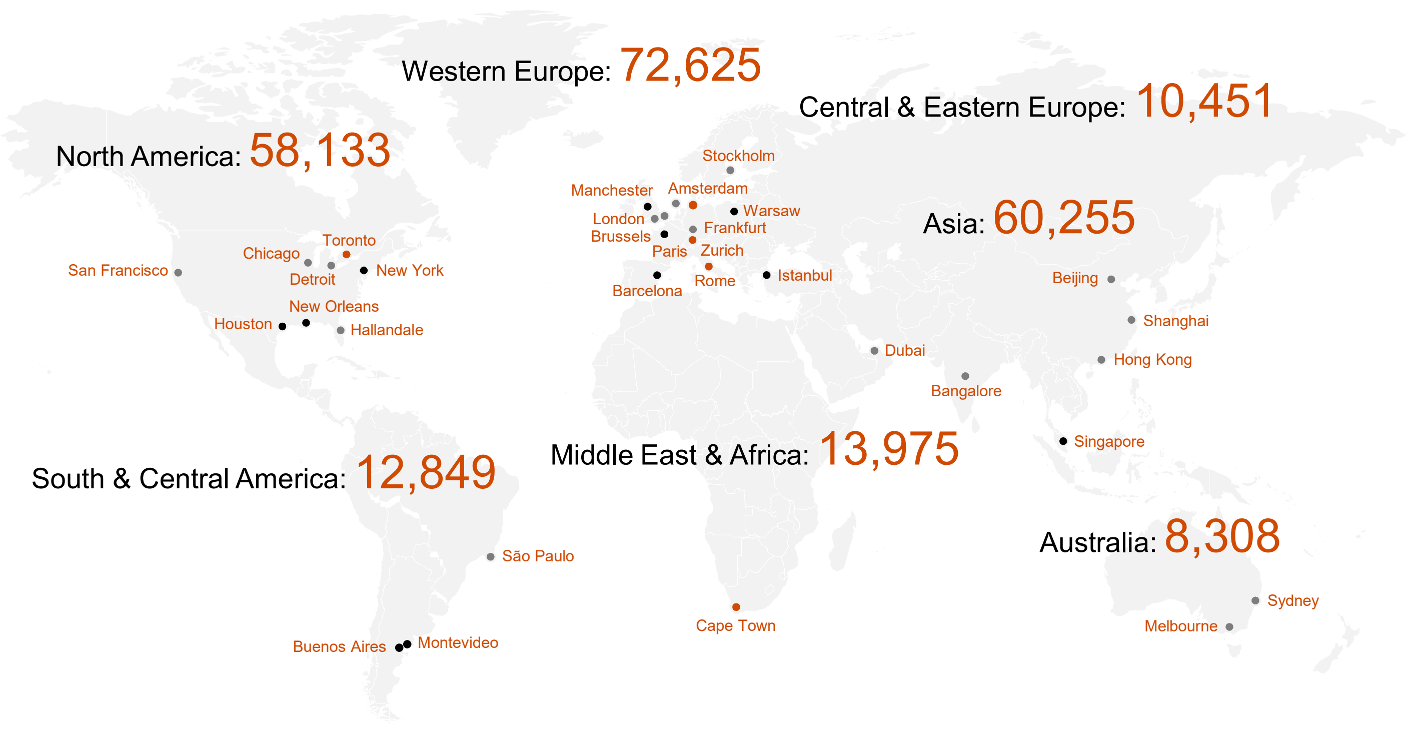
Average age 33

15 Locations

73 Nationalities

3300 Staff

Our trade and SAP experts are part of a global network that provides you with local expertise and industry best practices



• PwC Office • PwC Experience Center

284’000 – Overall number of PwC employees

PwC key facts

> 7,500 SAP professionals

> 550 Customs, trade, export controls & sanctions specialists

> 35 SAP GTS specialists

> 150 Countries

> 700 Locations

PwC Advantage

✓ PwC has a global alliance with SAP

✓ Ability to support worldwide in local languages and time zones

✓ Access to internal regulatory and transformational resources

✓ In-house digital services capability to enhance SAP solutions

2

Was bedeutet Trade Compliance

What is Trade Compliance ?

Focus area – for intangible goods

National and international treaties / regulations governing the movement of goods, software and technologies

There are two main reasons for a government to have export control regulations in place:

1. **Protection of national security** by restricting the supply of goods and technology for the purpose of:
   - Preserving national military superiority and ensuring the protection of the armed forces or their infrastructure,
   - Limiting the development of weapons of mass destruction, chemical or biological weapons, nuclear proliferation or items for internal repression or other serious human rights violations and the effects of terrorism.
2. **Respect for foreign policy** by :
   - Ensuring the support of allied countries,
   - Applying international agreements and treaties,
   - Following international boycotts or embargoes

Are subject to export control:

- **Products** (incl. models, demonstrators, prototypes...), their test / maintenance means (benches...), their hardware (PCB...) or software components
- **Software**
- **Services** (technical assistance, maintenance...)
- **Data & documents** (specifications, manufacturing and maintenance data...)

Exports can be carried out:

- By **tangible** means (shipments, mail...)
- By **intangible** means (e-mail, file downloads...)
- **Orally** (technical meetings, trade shows...)
- To a **foreign entity**
- To a **foreign or even national person** who is **not entitled** to receive controlled information.

Trade Compliance is an interdisciplinary task

People, Governance, Process and Technology

People

Sufficient resources with expertise to define requirements, implement controls, execute tasks.
→ A person holds the overall responsibility for compliance

Governance

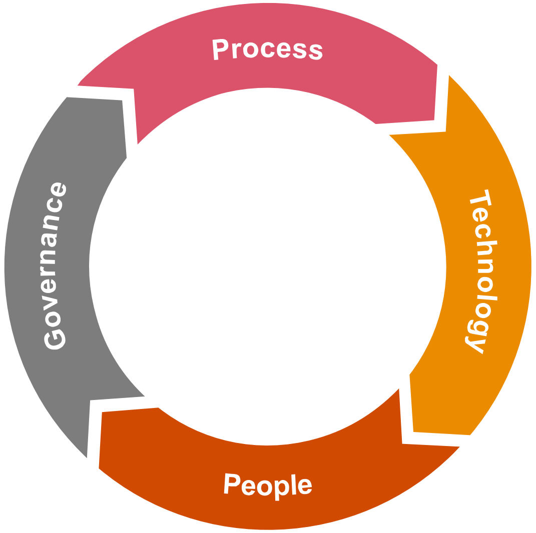
Defined roles and responsibilities to execute compliance relevant tasks by people following processes using technology

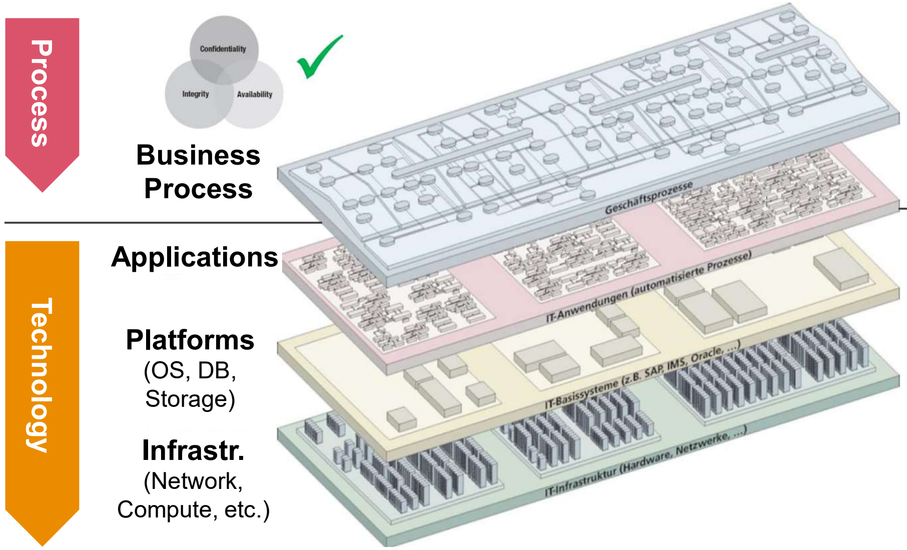
Process

Trade Compliance needs to be integrated in the supply chain and the business process landscape to identify, categorise and classify relevant (intangible) goods (information) subject to trade compliance and what measures need to be applied

Technology

This is the IT environment and Tool landscape that needs to support data protection, access control and accountability
→ who did what and when




Process
Confidentiality
Integrity
Availability
Business Process
Geschäftsprozesse
Technology
Applications
IT-Anwendungen (automatisierte Prozesse)
Platforms (OS, DB, Storage)
IT-Basissysteme (z.B. SAP, IMS, Oracle, ...)
Infrastr. (Network, Compute, etc.)
IT-Infrastruktur (Hardware, Netzwerke, ...)

IT & Tools are either in your Data Center or in the Cloud

Cloud vs Data Center

Dazwischen Präsentation – Export Controls & Cloud Computing von Harald Zimmermann

What is a Technology Control Plan (TCP)?

Focus area – information security plan for intangible goods

A Technology Control Plan is part of the Internal Compliance Program (ICP)

Why is a Technology Control Plan required?

Not only semi- and finished goods are subject to export controls, but also **software and technology.**

The **US, EU** and other export control regulations require a **Technology Control Plan** in order to **prevent unauthorised access** to and transfer of **information** that could be used for any kind of proliferation of weapons of mass destruction (WMD), targeted human rights violations, the threats of international terrorism or, by a foreign country to improve its missile or space launch capabilities.

What is understood as "information"?

Information can be **software, data, documents, services and technical discussions (Technical Data).**

A TCP consist of following elements:

1. Management commitment to export compliance
2. Physical security plan
3. **Information security plan**
4. Personnel screening procedures
5. Training and awareness program
6. **Self-evaluation program**

Scope of our presentation: This presentation covers **Information security plan,** as well as a **Self-evaluation apprach.** The control of any oral discussions or the physical export are excluded.

No	TCP Element	In scope / Out of scope
1	Management commitment to export compliance	✗
2	Physical security plan	✗
3	Information security plan	✓
4	Personnel screening procedures	✗
5	Training and awareness program	✗
6	Self-evaluation program and verification	✓

3

Der Technology Control Plan (TCP)

Deploying a TCP: includes this four key compliance measures

Goal: enable control of software and technology, and strict protection of technical data
Scope: Dual Use and Special Military Items → Rüstungsgüter (ITAR) in the other stream

1. Data Governance

Technical data must be **identified, categorised, classified** and **labelled (tagged)**

- Data Owner responsible for compliance
- Process (Lifecycle) to receive, allocate to a process step, and deliver / destroy the controlled item
- Legacy: already received data shall be rapidly sorted out to limit the risk of an export control violation
- “labelling” is a best practice. An alternative can consist in a systematic warning message

2. Data access restriction

CH, EU and controlled US technical data must be **Restricted** in logical access and manipulation (processing)

- The identify of all potential user needs to be defined and assessed
- Each User needs to have a defined “role” to assign access rights to the user role
- Access can only be granted as long as the individual needs to know and complies with citizenship/residency restrictions

3. Data transfer restriction

Technical data must be **controlled** and **tracked** for access and transfer (physical* or legal persons, citizenship/ residency permission)

- All accesses and transfers, whether by employees or sub/ co-contractors must be recorded/ controlled by the Trade Compliance Officer (TCO)
- This includes local IT and data centre or cloud / outsourcing
- Third parties who can access and manipulate the data shall be assessed and compliant to US and EU regulations (ex: IT Admin, sub/co-contractors, auditors…)

4. Access Control

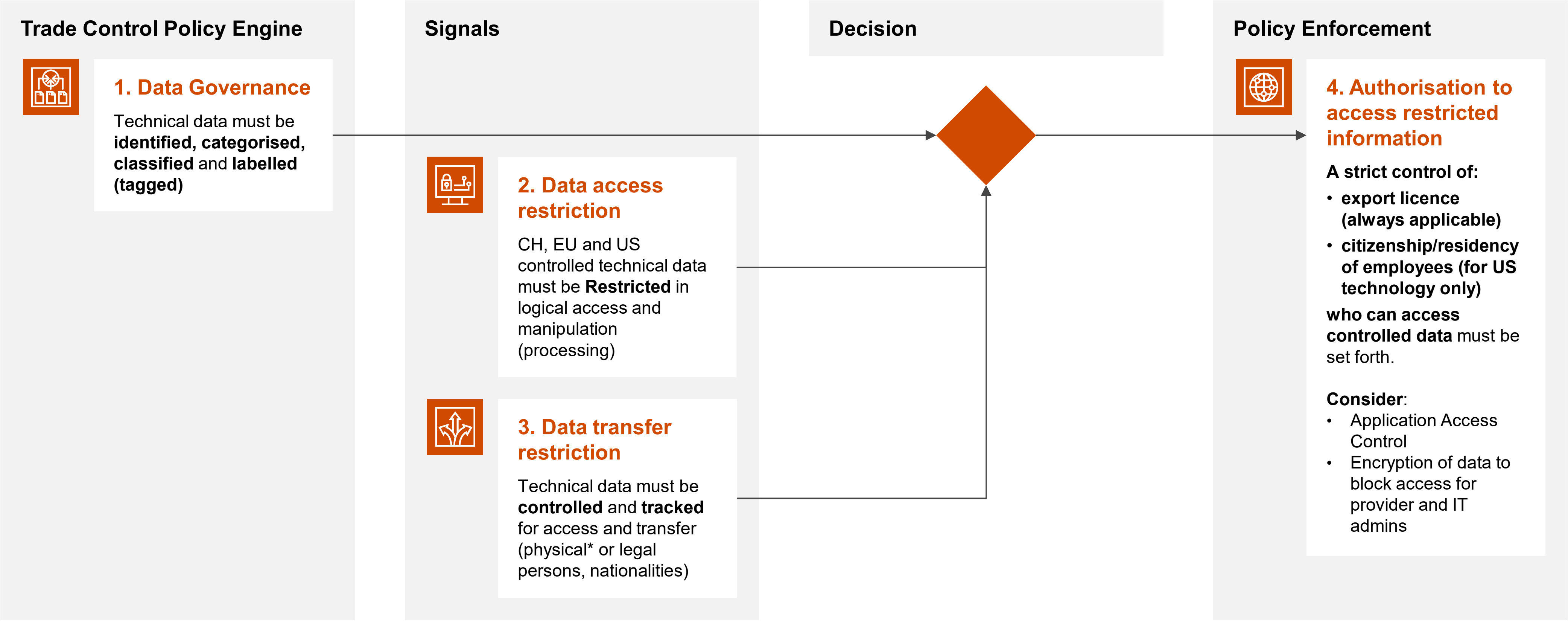
A strict **control** of **employees** (citizenship/ residency permission) **and subcontractors** who can access controlled technical data must be set up.

- Clients who need access to restricted information
- Employees working in the frame of a TCP shall be briefed (by the TCO) about the security measures and restrictions implied
- They shall formally acknowledge that the TCP has be presented to them and that they understood the TCP requirements.
- Entity shall keep records of acknowledgement

* Physical access controls are not part of this proposal

The first steps towards deploying a TCP – data governance

Define Data Ownership, categorisation & classification and how to control access



Trade Control Policy Engine

1. Data Governance

Technical data must be **identified, categorised, classified** and **labelled (tagged)**

Signals

2. Data access restriction

CH, EU and US controlled technical data must be **Restricted** in logical access and manipulation (processing)

3. Data transfer restriction

Technical data must be **controlled** and **tracked** for access and transfer (physical* or legal persons, nationalities)

Decision

Policy Enforcement

4. Authorisation to access restricted information

A strict control of:

- **export licence (always applicable)**
- **citizenship/residency of employees (for US technology only)**

who can access controlled data must be set forth.

Consider:

- Application Access Control
- Encryption of data to block access for provider and IT admins

* Physical access controls are not part of this proposal

Self-evaluation program

Checklist to verify that your TCP addresses all relevant and applicable requirements, is complete, in place and effective

1 Requirements

A User's Requirements document approved by Global Trade Compliance Officer

2 Architecture

An Architecture Engagement document covering Business / Functional / Data flows, solution alternatives, solution comparison, recommended solution, solution technical environment

3 Roadmap

An implementation approach and roadmap document

4 Solution Design

Licensing model & budgetary information from tool / platform vendors (high level cost of the proposed implementations)

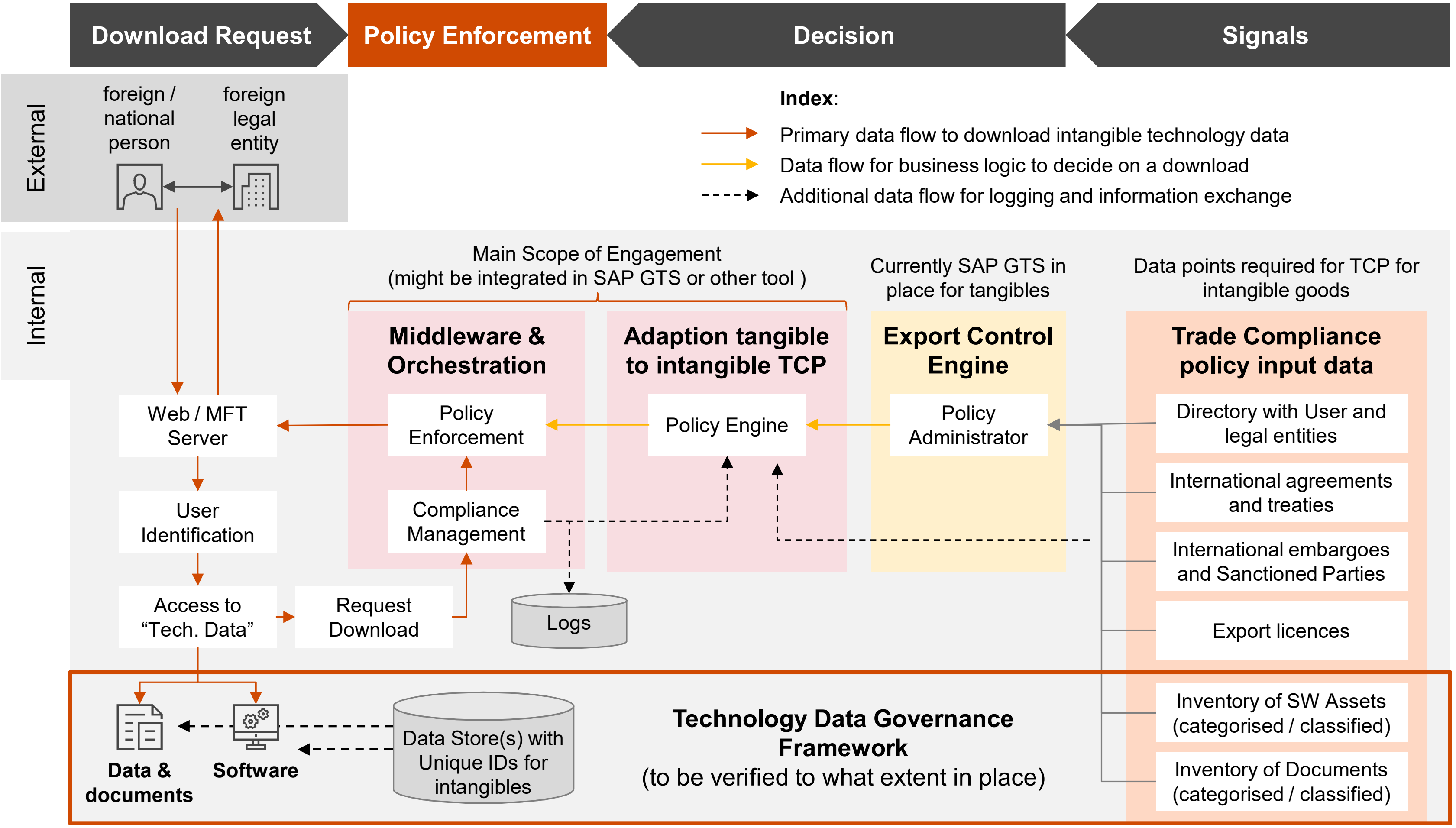
5 Implementation

Implementation plan according Roadmap as a project to change the business for upcoming transactions but also consider the legacy as a backlog

6 Verification

Verify that the defined controls of the TCP are in place and effective. Verify that you have evidences / audit trails for data classification, access and destruction

High level architecture blueprint– TCP for intangible goods


Download Request
Policy Enforcement
Decision
Signals
External
Internal
foreign / national person
foreign legal entity
Index:
Primary data flow to download intangible technology data
Data flow for business logic to decide on a download
Additional data flow for logging and information exchange
Main Scope of Engagement (might be integrated in SAP GTS or other tool)
Currently SAP GTS in place for tangibles
Data points required for TCP for intangible goods
Middleware & Orchestration
Adaption tangible to intangible TCP
Export Control Engine
Trade Compliance policy input data
Web / MFT Server
Policy Enforcement
Policy Engine
Policy Administrator
Directory with User and legal entities
User Identification
Compliance Management
International agreements and treaties
International embargoes and Sanctioned Parties
Access to "Tech. Data"
Request Download
Logs
Export licences
Inventory of SW Assets (categorised / classified)
Data & documents
Software
Data Store(s) with Unique IDs for intangibles
Technology Data Governance Framework
(to be verified to what extent in place)
Inventory of Documents (categorised / classified)

Architecture Building blocks

- **E.g SAP – GTS** is in place and has already the business logic to control tangible goods. Therefore, it is assumed that some/most rules can be re-used / adapted for intangibles
- **Adaption tangible to intangible** is a technical function to collect and normalize decisions enriched with additional signals to have a concise policy set for intangibles
- **Middleware & orchestration** acts as "policy enforcement" for the external access and request for downloads. It provides interfaces & security functions for "conditional access" and log transactions
- **Data Governance** enables you to identify and classify relevant technology data subject to TCP and steer decision for policy enforcement

Q&A

Questions and Answers

Thank you!

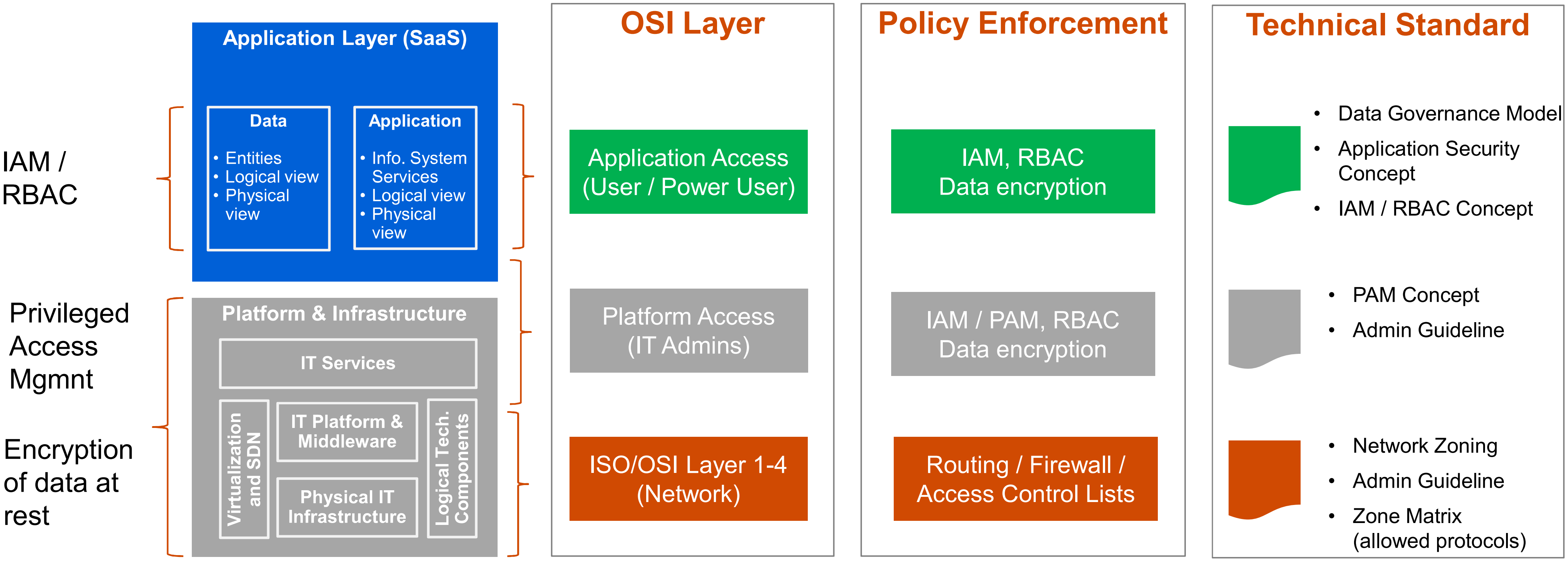
pwc.ch

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers AG, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2021 PwC. All rights reserved. In this document, “PwC” refers to PricewaterhouseCoopers AG which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.

Layered Security – multiple lines of defence

Before you can enforce a policy, you have to define the relevant technical standards



IAM / RBAC

Privileged Access Mgmnt

Encryption of data at rest

Application Layer (SaaS)

Data
- Entities
- Logical view
- Physical view

Application
- Info. System Services
- Logical view
- Physical view

Platform & Infrastructure

IT Services

Virtualization and SDN

IT Platform & Middleware

Physical IT Infrastructure

Logical Tech. Components

OSI Layer	Policy Enforcement	Technical Standard
Application Access (User / Power User)	IAM, RBAC Data encryption	Data Governance Model Application Security Concept IAM / RBAC Concept
Platform Access (IT Admins)	IAM / PAM, RBAC Data encryption	PAM Concept Admin Guideline
ISO/OSI Layer 1-4 (Network)	Routing / Firewall / Access Control Lists	Network Zoning Admin Guideline Zone Matrix (allowed protocols)