TADEUS

Improving Digital Security at European Tax and Customs Administrations

A review & recommendations - Final edition of the report from FPG 036

Foreword

The report you are reading is the outcome of FPG 036 on Digital Security. The project was created by TADEUS 2023 and has been led by the Swedish Tax Administration. The overriding aim of the project is to strengthen capabilities and resilience to threats within the area of digital security.

A team of IT-experts, specialists, managers and officers from 9 European Tax and Customs Administrations form the project group. All members of the project group have considerable experience and interest in the area of digitalisation and of digital security.

The project lead would like to direct a big thank you to all participants and others that have contributed to this report. The members of the group and their respective Tax Administrations are as follows:

Project lead

- Alexander Smith, The Swedish Tax Administration
- Peter Nordström, The Swedish Tax Administration
- Daniel Bynander, The Swedish Tax Administration

Participants

- Marcos Constantis, The Cypriot Tax Administration
- Jean-Marie Ulman, The French Tax Administration
- Sophie-Charlotte Wolf, The German Customs Administration
- Georgios Arsenis, The Greek Tax Administration
- Peter Bondár, The Hungarian Tax Administration
- Keith Redmond, The Irish Tax Administration
- Alessandro Cardillo, The Italian Customs Administration
- Peter Mikelj, The Slovenian Tax Administration
- André Javdan, The Swedish Tax Administration

Non-members of the project group assigned to the project by the Swedish Tax Administration include:

- Eric Stenberg, The Swedish Tax Administration
- Thomas Rönnerhed, The Swedish Tax Administration

2025-01-10 – Gothenburg, Sweden.

Index

1 Executive summary

Given the mandate in 2023 by TADEUS FPG 036 – Digital Security group was created to study four given subjects. The purpose of this report is to strengthen the knowledge of tax administration management and provide suggestions and recommendations on the given subjects

1. Digital Sovereignty
2. Harmonisation of standards
3. Co-location
4. Education and awareness raising

1. The project group recommends high level management to utilise the self-assessment tool developed by the project. The self-assessment tool is as close to a blueprint as possible. It includes the general ideas of digital sovereignty and supports administrations when choosing their own route to strengthening their digital sovereignty. A blueprint in its very nature is inflexible and ultimately demands that the administrations agree on a common definition of Digital Sovereignty, which the survey carried out by the project group found, they currently do not. By completing the self-assessment tool a benchmark will be obtained. This benchmark can be used prior to and during collaboration with peers. The outcome will also help top level management detect areas that may need strengthening such as data, information or technical sovereignty. Digital sovereignty is at the very core of Digital Security as it is the basis for how administrations take on the issue of Digital Security. By becoming aware and finding peers top level management will be well set for the next step; to strengthen their Digital Sovereignty so it matches their ambition.

2. Although there is considerable diversity in the way tax authorities apply their perception of digital sovereignty, and in the way their information systems are built, they all rely on suppliers of technological products and services. This dependence is even greater for technologies and skills linked to cyber defence. While there is a European framework, which is legal rather than operational, and European standards on cyber issues, tax authorities still have to turn to national standards, certification schemes and procurement practices when preparing calls for tender. The "One voice toward vendors" (renamed "Harmonisation of standards") subgroup explored these questions and identified opportunities through better sharing of the referable material already existing in member countries, and of identifying projects that tax administrations could work on together.

3. Emergency transfer of data will as the name suggests only become reality during a major emergency. What constitutes a major emergency that may force an administration to the extreme measure that transferring its crucial data to another location is hard to say. Events such as earthquakes, flooding, volcanoes, terror attacks and military invasions are examples of when data and information loss could become a reality. It is recommended that administrations do ask themselves the key questions provided in the questionnaire to assist them in evaluating their level of readiness.

Emergency transfer of data can be performed in different ways, from physically moving servers by rail, air or road to simply packing the data and uploading it into the cloud. The most cost-effective and practical way appears to be a hybrid solution, the combination of on premises solution and the cloud solution. Where to store the transferred data is the next part, trust is key when it comes to this. A crucial part of a successful emergency transfer of data operation is a trusted partner meaning that administrations need to both look at the technological and diplomatic side of things. Before the operational operations can take place agreements such as MOU need to be developed. If this was not enough, the whole operation has to be legal, not only with the national legislation of the sender but also of the receiver and other international bodies. The issue of emergency transfer of data is hard but not impossible to achieve. Crucial for smooth and cost-effective preparations is intra-administration cooperation. This could be accomplished by setting up a working-group with the task of sharing experiences and practices. As all countries have different levels of threat an alternative path could also be setting up a collaboration scheme with like-minded administrations that could advance at a higher speed than maybe a coalition of the unwilling might.

4. The report concludes by emphasising the importance of leveraging existing EU cybersecurity frameworks and educational initiatives. Tax administrations are encouraged to integrate awareness programs, ethical hacking practices, and security champions into their cybersecurity strategies. Furthermore, collaboration with ENISA is recommended to access resources that help in enhancing digital resilience.
   The focus on proactive measures, such as ethical hacking and security awareness, ensures that tax administrations not only comply with cybersecurity regulations but also adopt a forward-thinking approach to protect sensitive data. By investing in ongoing training and awareness, EU tax and customs administrations can mitigate the risks posed by evolving cyber threats, ensuring a secure digital environment for citizens and public institutions alike.

2 List of abbreviations

AD	Active Directory
AES	Advanced Encryption Standard
AgID	The Italian Digital Agency
ANSSI	French National Agency for the Security of Information Systems
AR-IN-A-BOX	Awareness raising in a box
AWS	Amazon Web Services
BCP	Participate in Business Continuity
BCRs	Binding Corporate Rules
BDSG	German Federal Data Protection Act
BMI	German Federal Ministry of the Interior and Home Affairs
CapEx	Capital Expenditures
CEH	EC-Council Certified Ethical Hacker
CER	Critical Entities Resilience
CISA	Certified Information Systems Auditor
CISO	Chief Information Security Officer
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Professional
COTS	Commercial off the Shelf
CRA	Cyber Resilience Act
CSIRT	Computer Security Incident Response Team
CSPs	Cloud Service Providers
DDoS	Distributed Denial of Service
DORA	Digital Operational Resilience Act (European Union)
DRaaS	Disaster Recovery as a Service
DRP	Disaster Recovery
DVS	German Cloud Strategy for Administrations
EDPB	European Data Protection Board
EECC	European Electronic Communication Code
ENISA	The European Union Agency for Cybersecurity
EU	European Union
EU5G	European cybersecurity certification scheme for 5G networks
EUCC	European Electronic Communication Code
EUCS	European Union Cybersecurity Scheme
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
ISACA	Information Systems Audit and Control Association
IS	Information System
IT	Information Technology
LED	Law Enforcement Directive
MLATs	Mutual Legal Assistance Treaties
MoU	Memorandum of Understanding
MSB	The Swedish Civil Contingencies Agency
NATO	North Atlantic Treaty Organisation

NIS/ NIS2	Network and Information Security Directive
OsiP	Open Systems Interconnection Protocol
OSS	Open Source Software
SAFE	Scaled Agile Framework
SaaS	Software as a Service
SCCs	Standard Contractual Clauses
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SLAs	Service Level Agreements
SSH	Secure Shell
TA	Tax administration
TLS	Transport Layer Security
VPN	Virtual Private Network
ZenDiS	German Centre for Digital Sovereignty of Public Administration

3 About the report

3.1 Background

The TADEUS (Tax Administration EU Summit) collaboration started 2018 and is a part of the Fiscalis programme of the European Union (EU). Fiscalis is an EU cooperation programme that allows Tax Administrations in each EU country to exchange information and experiences. It enables large trans-European IT systems to be developed and operated in partnership and to set up various personal networks by bringing together national officials from across Europe. TADEUS is a network in which the heads of tax authorities of EU countries work together with the Commission. Cooperation at operational and expert level already takes place within the framework of the EU-FISCALIS programme.

Nevertheless, this new form of cooperation at senior management levels was introduced to better address common challenges among EU countries in today's era of globalisation and digitalisation. The collaboration covers seven focus areas. One of these focal points is IT security. One issue that has grown in importance over the past decade concerns Digital Security. At the TADEUS meetings of the autumn of 2022 the need to strengthen all administrations awareness and capabilities in the area of digital security were acknowledged. The following winter TADEUS decided to create a project group assigned with the task of creating common conditions for establishing and securing the Member States capabilities concerning digital security.

3.2 The assignment

The mission originates from an agreement between the director generals of the EU Tax and Customs Administrations. The Swedish Tax Administration was appointed to lead the TADEUS project on digital security. Its main focus is on the public sector, especially the EU member states Tax and Customs Administrations, but can be useful to other administrations as well.

The assignment set by the director generals was to:

1. **Strengthen** the administrations digital sovereignty by creating a blueprint on how Tax and Customs Administrations can utilise the knowledge base (and perhaps IT-infrastructure) of other countries to help the tax and customs administrations strengthen their own resilience. The blueprint will support better understanding of the importance of the need for the Tax Administrations to become less vulnerable and more independent in the case of external threats to their respective IT infrastructure.
2. **Identify** where the participating Tax Administrations stand in their digital security procurement and, based on this, produce recommendations. The project should also aim at bringing forward the first parts of a harmonised requirement catalogue of what the tax and customs administrations current demands in the area are.
   What requirements do tax and customs administrations have on vendors? Can the biggest IT-vendors in Europe meet these requirements? Based on the answers to these questions create an account of the possibilities from the vendor's capabilities to deliver in accordance with the needs of the Tax Administrations.
3. **Establish** the first building blocks of future collaboration between member states regarding emergency transfers of data. The concrete assignment in this area to be undertaken by the project is to create a small case study looking at the following areas a. Legal possibility, b. Technical possibility, and c. Benefits and finance.

4. **Initiate** an education programme covering the knowledge security professional's need to be proficient in information security and IT-security. The programme should also aim at being able to identify how the fields are connected and their scope. An expected outcome of doing this is to achieve widespread knowledge at all levels of the Tax and Customs Administration of the current European IT-security education framework and it's availability to all member states.

3.3 The structure of the report

The report begins with an executive summary giving a quick overview of the assignment and recommendations. As quite a few sector specific words and abbreviations appear in the report a glossary and a list of abbreviations has been included in the beginning of the report, before the introduction, background and assignment.

The main part of the report is sectioned according to the four items of the assignment. Each item is presented in the same way,

1. Data
2. Considerations based on the data
3. Conclusions
4. Recommendations

3.4 An introduction to the content

All Tax and Customs Administrations are surrounded by a unique environment including threats and capabilities of defending its information and data. Each administration also has its own unique budget and set of national legislations giving it a frame of expenditure and room to manoeuvre. In a way these two items act as outer limits to what is possible to achieve in the area of Digital Security. For this reason, the conclusions, recommendations and examples presented in this report may not be completely feasible for all in their entirety. The purpose of them are nevertheless to strengthen the digital security and to increase resilience to cyber-threats. They are tools to support Tax and Customs Administrations but one should bear in mind that any actions taken based on them should be adapted to the unique operating environment.
The basis of the recommendations are the experiences and expertise of the members of the project group, their respective administrations and of some academic research.
Each of the four main chapters of the report can be read separately, but the reader is likely to obtain a deeper understanding by reading them all in order.
The last chapter includes thoughts and suggestions on how to follow up this report.

3.5 Methodology

The project group has used a hybrid style of work combining physical meetings, digital meetings, whole group discussions, smaller working groups and individual written contributions.

Information has mainly been collected from the countries represented in the project group but we have also included information from other organisations such as ENISA who joined us digitally at one of the first meetings. The aim was to secure knowledge and practical examples on initiatives undertaken, underway or under consideration. The members of the project group have discussed and reflected upon the differences, experiences, examples and strategies to increase knowledge and find some common understandings and challenges.

At the beginning of the project the ambition was to meet digitally at a regular basis. It soon became clear that the digital video meeting platforms available and tested never worked

satisfactorily for all members of the project group at the same time with at least 3-4 members having connectivity issues. For this reason the project group agreed on an alternative plan; dividing into sub-groups, arranging regular physical meetings and deadlines for written material to be submitted ahead of the physical meetings. The physical meetings were successful in fulfilling the ambitions of the project lead of establishing a forum for discussions and agreements of principle. Each and every member of the project group has in addition to being an active part of the physical meetings also produced the written content of the report. All group members have also partaken in sub-group meetings and discussions. The project lead strived to its utmost to accomplish the ultimate task of management and final delivery.

4 Digital Sovereignty

Sovereign = power without limit, fully independent and self-governing: having total power. Sovereignty = Independent sovereign power.[1]

4.1 Introduction

How do you evaluate your ability to control the data and information that belongs to you? Is your organisation in complete control of all your critical data and information? Does the physical location of the hardware containing your critical data and information matter? To what degree do you control the digital technologies that your organisation uses? These questions are all connected to Digital Sovereignty. The aim of the following texts and the exercises is to strengthen the organisation's capabilities to defend and maintain sovereignty and to open up for deeper collaboration with friendly minded neighbours to ensure mutual long term security for digitally stored and processed data and information.

The area of digital sovereignty is a fairly new concept. European countries today face threats not seen since the 1960's, but the threats of today are much more multidimensional. The kind of threats that countries and their public administrations face and the probability of different threats becoming reality differ from country to country. Present day threats could be traditional military force with occupation of territory as seen in the Ukraine. They could also be in the cyber domain as seen on a daily basis in Tax and Customs Administrations across Europe. Added to these are geopolitical movements closing borders, obstructing free trade, massive migration streams, attacks on supply chains, and huge electronic espionage by both states and large multinational companies.

To exemplify, the threat of military intervention is much higher in the European countries that border with Russia, but the threat of Russian intervention by other means is a reality for every country.

The different threats and the fact that European countries and their public administrations have vastly different backgrounds, history, culture and population influences the choices available with regard to digital sovereignty. For some public administrations it is better to keep their data close to heart and within its country's borders. For others it is better to hand over their data to a large corporation with superior resources compared to what the administration or even the whole country can provide. Sometimes a combination of internal and external Information and Communication Technology (ICT) operations is preferred.

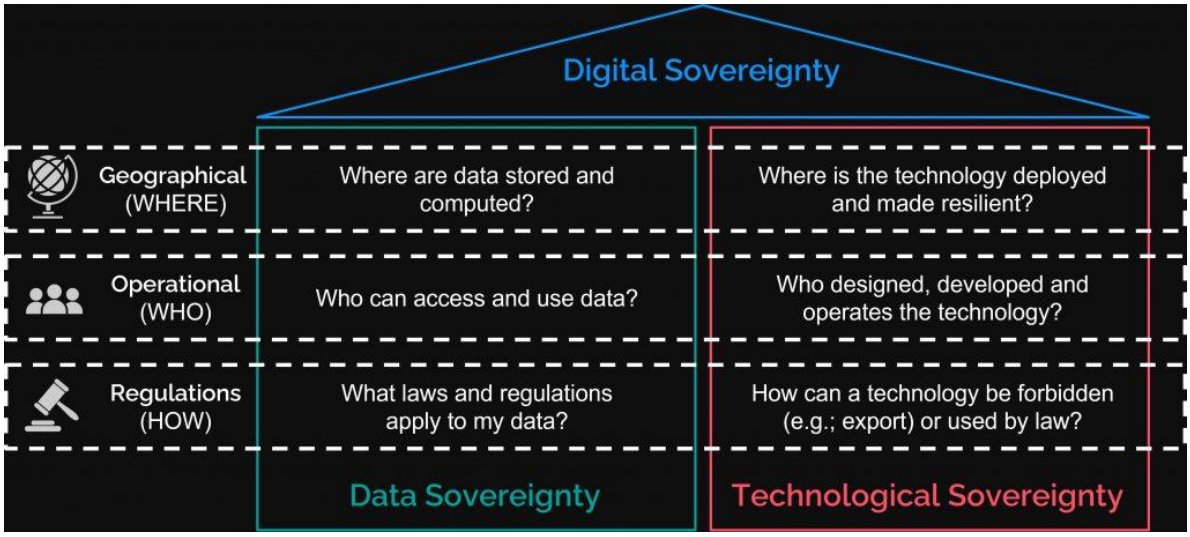
The most critical factor regarding digital sovereignty is complete control of critical information at all times. Other important factors impacting the level of digital sovereignty are technology, data, localisation and legislation.

There will be a brief highlight on data and information (4.2.1) as well as technology in a digital sovereignty context (4.2.2), the differences in the way European Tax and Customs Administrations currently define digital sovereignty (4.3), threats such as ransomware and cyber-attacks and counter measures such as ethical hacking (4.4), lessons learned from the war in Ukraine (4.5). The chapter ends with conclusions (4.6) and recommendations (4.7).

[1] Oxford Advanced Learner's Dictionary of Current English.. Fourth Edition. Chief Editor: A P Cowie. Oxford University Press 1989.

4.2 The different aspects of digital sovereignty

This diagram[2] created by the French IT company ATOS illustrates how Data and Technological Sovereignty can correlate towards Digital Sovereignty combining the geographical, operational and legal aspects. The diagram gives a good first look at the most important parts of Digital Sovereignty.



There'll be a closer look on data and information sovereignty and technological sovereignty in a digital sovereignty context in the following chapters.

4.2.1 Data & information

When discussing digital sovereignty it is essential to understand the differences between data and information.

Data can be described as a collection of facts and statistics. It is unorganised and without or with little context. It can be quantitative (numerical) or it can be qualitative (descriptive) but data will always be unprocessed. Examples of common data handled by a Tax and Customs Administration are:

- *number of visitors* the Tax Administration's website has recorded,
- completed *customs declarations*,
- completed *tax returns*,
- a *reply* to an enquiry from a tax officer or
- number of *incoming calls* to the Tax Administrations call centre.

Information is the result of analysing and interpreting data. It can be used to help making decisions. It is what data becomes when it has been processed. Examples of information common with European Tax and Customs Administrations are:

- customs officers *written responses* to incoming customs declarations,
- *notes* tax officers write regarding tax returns or
- *strategic documents* such as records of board meetings or the administration's risk analysis parameters.

[2] https://atos.net/en/lp/digital-sovereignty-cybersecurity-magazine/what-is-sovereignty-and-why-it-does-matter

In a digital sovereignty perspective information and data sovereignty refers to the degree of control the Tax and Customs Administration has over the information and data it produces, handles and works with. This refers to both information and data stored on a local server or online in a cloud. When it comes to sovereignty, knowing the location or whereabouts of the data and information is crucial.

European Tax and Customs Administrations have both European Union and national legislation to consider when handling, storing and processing information and data. When addressing data and information sovereignty issues, the administration therefor has to make sure that it complies with the current legislation.

A third important aspect of data and information sovereignty is access. In relation to location and legislation, knowing and controlling who actually has access to it and who uses the information affects the administrations Information and Data Sovereignty. Being in control of who accesses information and data is also likely to affect other aspects such as the level of trust the administration has amongst its stakeholders and the public.

Data and Information Sovereignty can be summarised by these three important questions taking in the geographical, operational and legislative contexts:

- *Where* is the data and information stored?
- *Who* can access and use the data and information?
- *What* legislation applies to the information and data?

4.2.2 Technology

Another fundamental aspect of Digital Sovereignty is technological sovereignty which can be best summarised as the degree of control the administration has over the technology it uses.

The location of the technological capacity of the administration determines how it can be deployed, it's resilience in the face of adverse events and protected from extra-administration activity. Common examples regarding the location of the technological capacity;

- The administration's technological *capacity is on site*.
- The administration has outsourced its technological capacity – the technological capacity is therefor on one or more *contractors premises*.
- The administration's technological capacity is on the *premises of another administration*.

Who designed and developed the technology together with who practically and theoretically operates it also affects the level of sovereignty, the capacity available to affect the operational side of the technology. In a theoretical sense sovereignty increases, if some or all of this capacity is "in-house". However, contracts with external parties giving the administration this capacity can work in a similar way.

There is also a legislative aspect to the technological side of Digital Sovereignty. European Union or national legislation decides what technology may be used and how.

Technological sovereignty can, just as with information and data, also be summarised by questions, taking in the geographical, operational and legislative contexts:

- At which *geographical location* is the technology being used and protected?
- Who sits on the *blueprints* of the technology?
- Who can *develop* the technology?

- Who *operates* the technology?
- What *legislation* applies to the use of the technology?

4.3 Defining digital sovereignty

The project group conducted a survey of how the participating administrations currently view the issue of Digital Sovereignty in general and their respective status. As the project group is a well-mixed deck of national Tax and Customs Administrations (all sizes and geographical locations), the survey is deemed to be representative enough for some general conclusions. The participating administrations submitted the following definitions regarding how they view, describe and define Digital Sovereignty.

4.3.1 The administrations of FPG 036 members definitions

A. Germany:

Digital Sovereignty describes the ability and capability of individuals and institutions to fulfil their tasks in a digital environment independently, self-determined and securely.

For this objective, the processing of the data necessary for the administration must be guaranteed using modern, functional and trustworthy information technology. This requires a transformation of public administration information technology with the aim of making it more independent of individual providers and products and increasing its resilience through the interchangeability of components.

Digital sovereignty means, in particular, creating alternatives and supporting and shaping an open, competitive market. This promotes innovation and flexibility in the IT of public administration - two important drivers of digitalisation in administration. Digital sovereignty therefore has the potential to accelerate administrative digitalisation.

B. Greece:

Digital sovereignty in a Tax Administration refers to a government's ability to exert control and autonomy over its digital infrastructure, data, and technology systems in the context of tax collection and management. It contains several aspects (nationwide or within the EU, depending on the context):

- *Data Control*: Ownership and authority over the data collected and processed as part of their operations and procedures.
- *Technology Independence:* A Tax Administration should not be extremely dependent on foreign technology providers or data storage services.
- *Cybersecurity:* There should be robust cybersecurity measures in place to safeguard against data breaches, cyberattacks and unauthorised access.
- *Expertise:* Skilled professionals within the country who can design, build, and manage digital tax systems in order to minimise dependence on foreign expertise.
- *Localisation:* Implement regulations that require the storage of certain tax-related data within national borders to prevent external bodies from accessing it easily.
- *International Cooperation:* It's important to balance all the above with international joint efforts. Tax Administrations need to adhere to international standards and treaties in order to facilitate cross-border activities and combat tax evasion effectively.

C. Slovenia:

Digital Sovereignty is the administration's ability to make independent and informed decisions regarding the use of digital technology and management of digital assets.

D. Cyprus:

For Cyprus Digital Sovereignty is the ability of our organisation to own and control its digital environment, respecting the data in its possession and providing at the same time the flexibility and agility to evolve throughout the time.

The Digital Sovereignty is defined and applied through our policies, procedures and culture.

E. Ireland:

States or organisations Digital Sovereignty include complete control of stored and processed data, as well as independent decisions of who may access this data. It also includes the ability to independently develop technical components and systems as well as changing, controlling and through other means complement these components and systems.

In the world of cloud computing and inter-dependability of countries for digital components (hardware, software, Operating Systems) the focus should be on the first part of the above and be on Data Sovereignty. Ultimately it is important to securely collect, store, use and protect data. While digital components are an enabler for this, we don't believe we can enforce a level of Digital Sovereignty and provide the required services needed.

F. France:

There is no definition of digital sovereignty specific to the Tax Administration.

Digital sovereignty has been talked about for over 20 years, but attempts to define it date back just over 10 years, when it began to be an element of public policy (under this name: the idea that computers and then networks were a key element of sovereignty and autonomy dates back to the 1960s).

A key definition of digital sovereignty is that it is "the State's ability to operate in cyberspace, which is a necessary condition for preserving our values. This implies both the ability to assess, decide and act autonomously in cyberspace and control over our networks, electronic communications and data".

Digital sovereignty can be seen as a filter applied to many areas (defence, continuity of the State, competitiveness, privacy, etc.) or technical fields (cloud, artificial intelligence etc.).

Although this is a simplification, digital sovereignty can be segmented into:

- *Legal sovereignty*: being able to define and defend an effective set of rules concerning what is essential to preserve the State and our values and to protect our citizens in the digital world; including what is necessary to maintain competitiveness and fiscal equity.
- *Data sovereignty:* being in control of the location, exposure and transfers of data relating to the functioning of the State, essential for the private sector or for citizens.

- *Technological sovereignty:* having the scientific, technical and industrial capabilities to protect the sovereignty of our data, defend ourselves in cyberspace and develop the digital economy.

The application of these principles to the Tax Administration is most obvious in three areas:

- *control over data and operations*: self-hosting and operation (historically, with some recent moves towards cloud offerings, mostly sovereign),
- *a technology mix* composed largely of open source solutions and platforms built in-house and
- *an own infrastructure*, tools and human resources to defend against cyber threats.

In recent years, the intention has been to examine the opportunities for using commercial off-the-shelf solutions (and even where there is no specific sensitivity extra-European solution). But this is associated with a relatively strict filter, when it could have an impact on essential missions, personal or economic information. For the Tax Administration, the evolutions should focus on those parts of the technology mix that address services to the end users and needs that can be addressed by COTS without exposing regulated or essential data.

G. Sweden

The Swedish definition of Digital Sovereignty includes complete control of stored and processed data, as well as independent decisions of who may access this data. It also includes the ability to independently develop technical components and systems as well as changing, controlling and through other means complement these components and systems.

H. Italy

Italy defines Digital Sovereignty with the following four points:

- *Data Sovereignty:* In Italy, access to public registers and confidential data is strictly regulated. Access is granted only to authorised personnel within government bodies and institutions. Security protocols and access control mechanisms are in place to ensure that only those with the necessary clearance can access this data.
  The Italian government exercises full control over the protection mechanisms of public registers and confidential data. They employ advanced encryption, regular audits and compliance with GDPR regulations to safeguard this data. The cybersecurity teams are continuously monitoring and updating our security protocols to protect against emerging threats.
  The control of public registers and confidential data lies with specific government departments and agencies under the supervision of the Ministry of Innovation and Digital Transition.[3] These entities ensure that data management practices align with national security and privacy standards. The Italian Digital Agency - AgID - provides comprehensive cybersecurity guidelines for public administrations, which the ADM strictly follows.[4]
- *Technology:* Many of our critical network and infrastructure components are owned and managed in-house by a private state-owned company – Sogei S.p.A. - to maintain higher security and control. Certain non-sensitive infrastructure components are shared with other administrations to optimise resources and enhance inter-administrative collaboration. We utilise outsourced technology for non-sensitive data storage and processing. Stringent

[3] https://innovazione.gov.it/dipartimento/en/structure/

[4] https://www.agid.gov.it/

contracts and regular audits ensure that these service providers comply with our data sovereignty requirements.
With regards to localisation, the primary data centres for sensitive data are located on government premises, ensuring direct control and enhanced security measures.

- *Localisation:* For co-located nation-wide data centres, Italy is fully aware of where our data is located and maintain detailed records of the locations and access permissions. Regular audits and security checks are performed to ensure data integrity and security.
  Italy has started using cloud solutions in recent times (mostly provided by Microsoft) and ensures that the service providers adhere to the Italian data sovereignty policies. Italy also have detailed records and control mechanisms to track where and how data is processed, ensuring compliance with their sovereignty standards. Cloud Service Providers (CSPs) must obtain certification through the AgID Cloud Marketplace, following AgID guidelines.
- *Information and output:* Regarding the protection of the production of data, Italy has implemented stringent security measures, including encryption, access controls, and secure communication protocols to protect the data production process. Decision-making is informed by regular risk assessments and security audits. The integrity of information is secured through the use of advanced encryption technologies, real-time monitoring and robust access control mechanisms. We also enforce strict compliance with national and EU-wide data protection regulations. Italian data sovereignty is maintained during inter-departmental cooperation in everyday operation by using secure collaboration tools and encrypted communication channel.
  Italy collaborates with CSIRT Italy (Computer Security Incident Response Team) to share threat intelligence and incident information.[5]
  Automated systems, especially in the anti-fraud sector, are designed with sovereignty in mind ensuring that any checks and analyses performed on the data comply with the security and sovereignty policies.

4.3.2 A comparison of the definitions

It is obvious that the participating administrations look at Digital Sovereignty differently. The definitions of what is regarded as Digital Sovereignty vary and there are also quite a few similarities. The members of the project group found that the definitions vary to such a degree that agreeing on a common definition is not possible at the present-day. The administrations, and in a sense the nation states, are currently too far away from each other in the matter, that agreeing to or publishing a shared definition seems not conceivable. However, the participating administrations do appear to agree on the importance of information security and being in control of ones executive decision making.

For instance the Swedish Tax Administration defines Digital Sovereignty as being in complete control of stored and processed data, as well as independent decisions of who may access this data. It also includes the ability to independently develop technical components and systems as well as changing, controlling and through other means complement these components and systems.

The Cypriote Tax Administration's definition also includes the ability to own and control its digital environment and the data it handles. It also stresses the need to be able to evolve but steps short of defining who or where the technical development should proceed.

[5] https://www.csirt.gov.it/

Irelands Tax Administration on the other hand shares most of the Swedish definition, but finds that in the world of cloud computing and inter-dependability of countries for digital components the focus should be on the first part. Ireland notes that the most important thing is to securely collect, store, use and protect data. While digital components are an enabler for this, the Irish Tax Administration does not see that it can enforce a level of Digital Sovereignty in the technological area as it is hard to provide the services necessary.

The Slovenian Tax Administrations definition stops at its ability to make independent and informed decisions regarding the use of digital technology and management of digital assets.

The German Tax Administration describes digital sovereignty as the ability and capability of individuals and institutions to fulfil their tasks in a digital environment independently, self-determined and securely. The German Tax Administration also notes that the processing of the data necessary for the administration must be guaranteed using modern, functional and trustworthy information technology and that this requires a transformation of public administration information technology with the aim of making it more independent of individual providers and products and increasing its resilience through the interchangeability of components. Germany hereby includes the need for control over the physical hardware in the definition of digital sovereignty, as does the other two large administrations partaking in the project, the Italian Customs Administration and the French Tax Administration.

The Italian Customs Administration has established practices and taken action accordingly in the main areas of Digital Sovereignty. A major reason for this is the Italian government's centralised decision making in the area, but also the Italian state's financial and technical capabilities in the area which supports the national administrations. Examples of this is that the Italian Customs Administration owns critical network and infrastructure components and manages these in a separate state-owned company in order to ensure and maintain higher security and control. Additionally with regards to localisation, primary data centres for sensitive data are located on government premises, ensuring direct control and enhanced security measures.

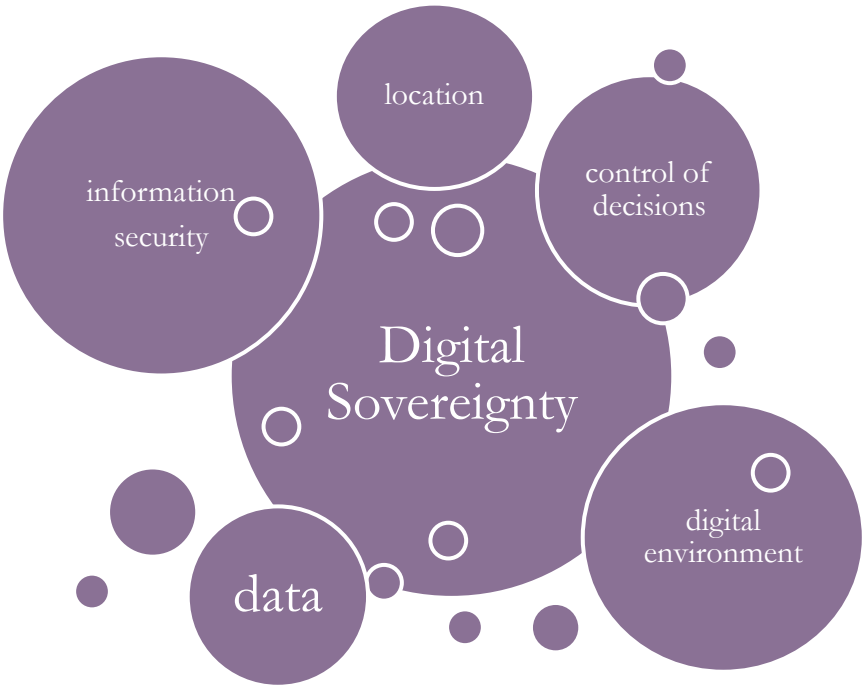
The French Tax Administration does not have an independent definition of digital sovereignty, but shares the definition set by the nation state. This definition is vast and includes a total perspective both data and technological sovereignty. It includes not only the physical hardware but also the capability to some degree produce or repair the physical hardware. For the Tax Administration this implies control over data and operations meaning self-hosting and self-managed operation, a technology mix composed largely of open source solutions and platforms built in-house with its own infrastructure, tools and by its own human resources. The Tax Administration's aim and purpose for this is to defend itself against cyber threats.

Once all the definitions had been analysed and discussed, all administrations vary to some degree on the issues of data, localisation, control, storage, hardware and IT-services.

As noted above, there are considerable differences, but there is also one important similarity that unites the participating administrations: The aim to maintain the ability to make independent decisions.

When summarising the differences and similarities, a slanting scale can be distinguished putting the larger administrations. These include control of both software and hardware in their definitions. Smaller administrations include fewer aspects, but critically aim to maintain control of information and data, some even only the bare minimum such as their ability to make independent and informed decisions.

It appears that all administrations more or less agree on the need for data and information sovereignty, but to a lesser extent to technological sovereignty.



4.4 Ransomware and Cyberattacks

Taking measures regarding data Sovereignty in particular is important when preventing Ransomware and Cyberattacks. A high level of technological sovereignty could further enhance sovereignty by making it harder to attack you.

4.4.1 Defining Ransomware and Cyberattacks

A. Ransomware

Ransomware is a type of malware that permanently blocks or limits someone's access to their systems and or data, either by locking the system's screen or by locking the files until a ransom is paid. More modern ransomware families, collectively categorised as crypto-ransomware, encrypt certain file types on infected systems and force users to pay the ransom through certain online payment methods to get a decryption key.

The motivation behind ransomware is often financial gain, but it's also known to be used by state actors to hide or disguise other cyber-attacks or information retrieval attempts. The groups creating ransomware are often linked to organised crime and certain countries such as North-Korea and some former Soviet republics.

Ransomware often spreads in an organisation or through their vendors or contractors or other external partners by phishing emails or by giving external party's access to certain parts of the IT-environment.

In January of 2024 many Swedish companies, universities and government agencies and municipalities were affected by a ransomware attack against one of the largest vendors in Sweden. Many of the customers system and data was inaccessible and work is ongoing at the

time of writing to restore and save the affected organisations data. The attack was intended to have as large an impact as possible and therefore aim at strategic links. The perpetrators are often interested in affecting many organisations with the goal to ensure that enough of them pay the ransom fee. This is why it makes sense for the attackers to hit providers of IT-services and not specific organisations. They also often exploit common of the shelf equipment that is used by many vendors.[6]

B. Cyberattacks

A cyberattack is a malicious and deliberate attempt to breach the information system. A cyberattack is always carried out by a person or an organisation on another person or organisation. Many large organisations are victims of cyberattacks. The motives for an attack can vary but attacks carried out on large organisations are usually either to gain financially or for political reasons or both.[7] The reason for conducting a cyberattack is to seek a benefit from disrupting the victim's network.

4.4.2 Ethical hackers

Ethical hacking, often associated with white hat hackers, is a critical component of modern cybersecurity. Unlike their malicious counterparts—black hat hackers—ethical hackers use their skills to enhance security rather than exploit vulnerabilities. Their primary goal is to identify and address weaknesses before they can be exploited by cybercriminals, contributing significantly to the overall security framework of organisations and systems.

Ethical hacking involves the practice of deliberately probing and testing computer systems, networks, and applications for vulnerabilities. This process is conducted under authorised and controlled conditions, with the express permission of the system owner. Ethical hackers use the same techniques and tools as malicious hackers but do so to uncover and fix security flaws rather than to exploit them.

The practice of ethical hacking is guided by a code of conduct and a set of professional standards. Ethical hackers, often referred to as white hat hackers, follow legal and ethical guidelines, ensuring their activities are both authorised and beneficial. Their work involves a range of activities including vulnerability assessments, penetration testing, and security audits.

White hat hackers play several crucial roles in the cybersecurity landscape:

- **Vulnerability Identification:** One of their primary responsibilities is to identify security vulnerabilities in systems, applications, and networks. By conducting penetration tests and vulnerability assessments, they help organisations discover weaknesses that could be exploited by malicious actors.
- **Risk Mitigation:** Once vulnerabilities are identified, ethical hackers work with organisations to address and mitigate these risks. They provide detailed reports and recommendations for strengthening security measures, such as patching software, configuring firewalls, and enhancing security policies.
- **Security Awareness:** White hat hackers contribute to raising security awareness within organisations. They often conduct training sessions and workshops to educate employees

[6] https://www.asperiq.com/article/ransomware-attack

[7] https://www.wired.com/story/the-us-government-has-a-microsoft-problem/

about common threats, safe practices, and how to recognise phishing attempts or other social engineering tactics.

- **Compliance and Regulation:** Many industries are governed by stringent security regulations and standards. Ethical hackers assist organisations in meeting these compliance requirements by ensuring that their systems are secure and that they adhere to industry best practices.
- **Incident Response:** In the event of a security breach, ethical hackers can play a vital role in the incident response process. They help analyse the breach, understand how it occurred, and develop strategies to prevent future incidents. Their expertise is crucial for minimising damage and restoring normal operations.

The importance of white hat hackers cannot be overstated. Their work helps to:

- **Pre-empt Cyber Threats:** By identifying vulnerabilities before malicious hackers can exploit them, ethical hackers help prevent potential breaches and attacks. This proactive approach is essential for safeguarding sensitive information and maintaining the integrity of systems.
- **Strengthen Security Posture:** Regular penetration testing and security assessments by ethical hackers contribute to a robust security posture. They help organisations stay ahead of emerging threats and adapt their security measures accordingly.
- **Enhance Trust and Reputation:** Organisations that invest in ethical hacking demonstrate a commitment to security and risk management. This can enhance their reputation and build trust with clients, customers, and partners, knowing that their data is protected.
- **Support Continuous Improvement:** The cybersecurity landscape is constantly evolving, with new threats and vulnerabilities emerging regularly. White hat hackers provide valuable insights and feedback that support continuous improvement and adaptation of security strategies.

Ethical hacking is integral to the broader concept of cybersecurity. It provides a crucial layer of defence by ensuring that security measures are tested and validated from an attacker's perspective. This practice helps organisations identify gaps in their security architecture, develop effective countermeasures, and maintain a proactive stance against cyber threats.

Moreover, ethical hackers often collaborate with other cybersecurity professionals, such as incident responders, forensic analysts, and security architects, to create a comprehensive security strategy. Their contributions help build a culture of security awareness and resilience within organisations, ultimately leading to a more secure and trustworthy digital environment.

In conclusion, ethical hacking and the role of white hat hackers are vital components of a comprehensive cybersecurity strategy. Their expertise in identifying and addressing vulnerabilities, coupled with their commitment to ethical practices, plays a crucial role in protecting organisations from cyber threats and ensuring the overall integrity of digital systems.

4.4.3 Considerations Ransomware and Cyberattacks

One of the weakest links in the protection of an organisations data and information is the awareness regarding potential consequences to slack behaviour by the users. The importance of raising awareness at all levels is critical to prevent infection spread from for instance phishing e-mails or infected USB devices.

Threat intelligence, protection of information through encryption, backups that are kept offline are other measures on a technical level that ensure the resilience of organisations against ransomware.

The risk of being affected as collateral is higher when ones data is shared with others that may be affected, however this must be put into contrast to the availability and possibilities for each member to handle an attack and protect ones data. Many of the topics discussed in this report point at this and need to be carefully considered by each organisation according to their needs and feasibility in creating resilient cyber security.

Organisations that use alternative high-assurance products not only enjoy the high assurance as such, but also do not run the risk of becoming collateral damage to sweeping attacks that target common commercial products.

Unfortunately, there is no silver bullet to address the ransomware threat as a whole, but the key is to construct multiple layers of defence to reduce the risk of being compromised.

In the light of the above, organisations therefore need to make a decision on what level of sovereignty is enough for them given cost and risks. To share infrastructure with others could, if lacking appropriate measures and demands on the vendor in fact lead to higher risks of being affected by ransomware. If the decision is made, with enough information the appropriate methods of protection can be taken.

4.5 Ukraine as an example for the significance of digital sovereignty

In an effort to visualise the importance of digital sovereignty and digital security here's the most important current event in Europe as an example. It is there to raise questions on what measures can be taken to protect the sovereignty and what threats and consequences there could be if assets and data are not properly secured.

4.5.1 Cyber-attacks and counter measures

In 2023 the Swedish Civil Contingencies Agency (MSB) published a report[8] on lessons learned from the non-military defence of Ukraine during the Russian invasion. One of the topics studied was cyber and information security.

In 2014 Russia annexed the Ukrainian region of Crimea. On the 24th February 2022 Russia initiated the large scale invasion of Ukraine. The invasion has resulted in many casualties. Apart from the humanitarian suffering, the Ukrainian society also suffered from attacks on energy infrastructure, food supply and access to public services.

The years following the annexation of Crimea, Ukraine experienced several Cyberattacks. By learning from these experiences, Ukraine introduced targeted cyber-defensive measures and has been able to withstand many of the attacks thrown at it lately.

During the first six months of the invasion, more than 1500 cyberattacks were targeted at Ukraine, half of which were performed during the first months of the large scale invasion. The purpose of the attacks was to hinder civilian and military organisations in Ukraine from functioning, directly damaging the Ukrainian society and gaining advantages for the Russian military.

[8] https://www.msb.se/contentassets/5d70a3f1096d46348e1ae3acf257689c/fo2023-01325-erfarenheter-fran-ukraina_initiala-lardomar-for-det-civila-forsvaret.pdf

Information that is available today shows that Ukraine has been successful in preventing the majority of attacks. Since the conflict is ongoing, the true extent of damage caused by Russian cyber and information attacks can be difficult to assess as well as the true extent and damage caused.

Russia used different techniques during the initial phases of the invasion. In the early stages of the invasion the methods used where more sophisticated, for example attacks on satellite-based networks. The period following the first stage of the invasion contained more primitive attacks such as Denial of Service attacks and phishing. Both sides appear to continue to learn, adapt and develop which could result in more advanced attacks in the future.

Sensitive government information was at risk of being lost to the aggressor during the invasion. After the annexation of Crimea Ukraine had moved all its data from the regions to servers located in Kiev. Prior to the invasion, Ukraine strengthened the security surrounding of these servers and also implemented protections against unauthorised deletion of data, if the servers where to fall in the wrong hands. Ukraine prepared a back-up plan for parts of the most essential data that could be activated on different geographical locations in case Kiev was lost to the aggressor.

Ukraine, just like many other countries in Europe and around the world, did not allow for data and information to be processed outside of their own borders. Just one week before the invasion, their parliament enacted a law that allowed for the government to move sensitive data to cloud-services even though the servers where located outside of Ukraine.

With the help of private entities, parts of the government's digital infrastructure could be moved outside of Ukraine. Privately owned companies and civil society organisations also received support in moving their services and data.

4.5.2 'The IT Army of Ukraine'

Some privately owned companies complemented the state's effort and provided additional support aimed to lessen the impact of the Russian cyber and information attacks.

One example often raised as a success in Ukraine's ability to withstand the attacks from Russia is the formation of the "IT Army of Ukraine". The army is made up by a group of volunteers that attack Russian assets. Even though the group is not officially supported by the Ukrainian government, it has made an impact in reporting Russian troop movement and airborne threats in occupied areas. An effect attributed to this effort is a sense of participation and of strengthening the public will to defend the nation. The effort also shows the flexibility and high degree of resistance against the aggressor. [9]

4.5.3 Lessons learned from Ukraine

In regards to cyber security and the ongoing war in Ukraine, some key points can be of value to all organisations:

- Work long term using an *"all-risk" perspective*. To be resilient you need to have a high level of both information and cybersecurity.
- A future scenario is that the cyberattacks are more sophisticated and will occur ahead of physical attacks. It is therefore important to *plan and prepare* for a different attack vector.

[9] https://www.msb.se/contentassets/5d70a3f1096d46348e1ae3acf257689c/fo2023-01325-erfarenheter-fran-ukraina_initiala-lardomar-for-det-civila-forsvaret.pdf

- *Sovereignty* is important both in terms of ones control of information but also different IT-resources. *Legal considerations* need to be made in regards to both national as EU law.
- *Secure storage* of sensitive and important information to prevent information loss and to keep data that is important for society to work. *Control* over how and where your information is stored is critical.
- Make demands on functions that need to be available in a time of crisis and follow up on those demands. The *awareness* of IT-incidents and cyberattacks also need to be raised.
- Secure *digital supply* and how information flows between different actors. Take measures to not be overly dependent on one part or vendor.

Many of the lessons learned and recommendations are things that we do or should do in the scope of working with digital security.

Be aware of:

- our *information* and how to *protect* it.
- the *ever changing threats* that are emerging and take appropriate measures. These measures can be different depending on the context.
- making *conscious decisions* on what measures and risks are acceptable given the sensitivity and consequences of potential data loss or denial of access to data and information.

4.6 Conclusion Digital Sovereignty

The current status and evaluation of choices concerning Digital Sovereignty have to be conscious and motivated. This enables an organisation to enact the necessary safety procedures according to their capabilities and needs, thereby ensuring the safety of the valuable information it manages for its beneficiaries. A conscious and motivated stance regarding Digital Sovereignty is also a requirement for collaboration with other administrations, domestic or international.

When analysing the different definitions of digital sovereignty, value can be created by highlighting the diverse approaches the member states display on the topic as well as other data, such as reports written by other organisations and IT-security analysts.

The take-away is that is complex and in some degree different for each administration. The core business of governmental power is how administrations handle information and data and that is why methods to define administrations sovereignty are needed.

The first step on the challenging path of maintaining digital sovereignty is to become aware of one's current status in the four main areas: *data, localisation, information and technology*. In order to achieve this, a guideline has been developed on how to perform a self-assessment (Appendix 1). The self-assessment guideline can be used to identify an administrations current stance. It can also be used as a stepping stone towards a point where an administration can begin to discuss its standings amongst its peers. The result can also be used as an enabler of further collaboration at an international as well as national level and for future solutions to common threats within the scope of digital security.

4.7 Recommendation - Digital Sovereignty

The self-assessment aims to help identify an administration's current position regarding its digital sovereignty. Being aware of where one's administration stands at the present is crucial

for high level decision making. Only when the administration's current stance is clear to the decision makers they can take the right action at the right time.

The self-assessment tool can also be used when looking at different scenarios such as war or natural disasters.

The greatest benefits from performing the digital sovereignty self-assessment are:

- *identifying security measures* the administration currently lacks,
- gaining information that may be used as a base for *future collaboration* with other administrations and organisations at a national as well as an international level and
- obtaining a *benchmark*.

It is vital for all organisations to have complete sovereignty over the information area. The other three areas are also very important, but not vital to have complete sovereignty over. It is more essential that you can explain and motivate yourselves and your stakeholders, why you have chosen a certain level of sovereignty. The recommendation is to, at the very least, reflect over the current level of sovereignty and you would like to have for each area.

The questions seen in the self-assessment tool are examples that, when assembled, will give you a good view of your current level of digital sovereignty, they are neither comprehensive nor are they compulsory. How they are answered will give you a general direction, but the answers on their own are by no means a base big enough for a complete conclusion. They provide an important part in raising awareness and understanding digital sovereignty.

5 Harmonisation of standards

In the context of this report, vendors are identified as those that provide IT solutions or manpower that either directly address cybersecurity subjects or have a direct impact on the ability to operate in a continued (and for some a sovereign) way when exposed to territorial or cyberspace attacks.

This section explores the existing tools at European or Member State level that contribute to obtaining more relevant offers from vendors, then attempts to identify specific areas where a more coordinated approach toward vendors is especially needed, and finally proposes an approach both to address the most critical areas of digital security through procurement, and to better identify useful collaboration areas in the future.

5.1 Introduction

Discussions around the concept of digital sovereignty have highlighted differences between member states, in the perception of what it covers, and in sensitivity towards the use of solutions that are more or less sovereign.

Above all, they have highlighted the fact that an information system, in this case that of a tax authority, cannot be designed in a vacuum and relies for its construction on suppliers of hardware, software, software as a service (SaaS) and IT services. Some European, others not. All of them having a profitability issue at stake, which for most of them tends to lead to unified rather than adapted responses:

- this is very true for an IT hardware supplier, for example, who will find it difficult to specialise to meet the specific needs of a given customer
- this is also very true for infrastructure services (cloud) and software as a service (SaaS) suppliers
- it may be marginally more flexible for some specialist software, but certainly not for software that meets generic needs (digital work environment for example)
- it is not so true of IT services, which may be less difficult to adapt to local needs, at the possible cost of an heterogeneous quality, depending on the sophistication of the requirements expressed by each customer.

Among these offers, those that contribute most directly to the continuity of service of tax information systems, to resilience in the face of the cyber threat, and to the defence of European interests against non-European players, are particularly relevant to address in a coordinated manner:

- at least because, to cover a given need, the same requirement applied by all the tax authorities will be less costly to produce, and therefore to acquire, than a variety of similar but incompletely convergent requirements,
- more so because in many cases, the interest for vendors in producing an offer that meets a set of local requirements will be insufficient to justify the effort, and there will be no appropriate response or only a partial response,

- clearly too because, for the Tax Administrations, it is a non-trivial and costly thing to define sets of requirements, standard, certification scheme, etc. sufficient to ensure a given quality from vendors, notably of IT Services.

5.2 Existing European standards and initiatives

Resilience and improving the level of cybersecurity in the European Union has been a significant subject in recent years, leading to the publication of several broad directives or declarations, of which the most significant are probably:

- Directive (UE) 2022/2557 on the resilience of critical entities,
- Directive (UE) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2),
- Regulation (UE) 2022/2554 on digital operational resilience for the financial sector (DORA),
- Regulation (UE) 2022/0272 Cyber Resilience Act (CRA),
- Regulation (EU) 2019/881 The EU Cybersecurity Act etc.

Most of those legal texts are only superficially actionable to address vendors. NIS 2 or DORA (when applicable to tax administrations, specifically for banking activities) can at most help enrich operational clauses for contracts, but they are far from being specifications or technical standards. CRA is more geared toward the consumer market, and although there exist an attempt at mapping its requirements to existing standards[10], it's too fragmented and convoluted to be of direct use.

5.2.1 Cloud services

Cloud hosting and services, which are an essential component of any IT strategy, even more so as a mean of addressing a risk on physical / territorial sovereignty, are the subject of quite a lot of EU initiatives, at least four of them addressing cybersecurity:

- The Data Act (Regulation (EU) 2023/2854),
- The EU Cloud Code of Conduct (https://eucoc.cloud/),
- The EU Cybersecurity Certification Scheme for Cloud Services (EUCS),
- The EU Cloud Rulebook.

The Cloud Code of Conduct is of particular interest as a framework for cloud service providers to demonstrate compliance with the GDPR. It does not directly specify cybersecurity measures but references specific control points in external standards. It does not addresses resilience or sovereignty.

The most promising initiative from a procurement point of view is the work in progress on EUCS. EUCS is being elaborated by the ENISA in compliance with the Cybersecurity Act (Regulation (EU) 2019/881). The EUCS includes detailed technical and operational requirements that contributes to make it relevant to reference as a synthetic standard for procuring a cloud service.

[10] https://www.enisa.europa.eu/publications/cyber-resilience-act-requirements-standards-mapping

Still, as of the writing of this report, there is a significant issue with regard to EUCS and its ability to protect data and operations against extraterritorial interference. The latest version of the EUCS, proposed by the ENISA, while still addressing the technical aspects of offering a cloud service, removes all the clauses that would protect cloud hosting against predatory legislation (e.g. the US Foreign Intelligence Surveillance Act or China's National Intelligence Law). Depending on what happens next, EUCS will need complementary clauses on compliance to vulnerabilities due to legal aspects. Otherwise, it might not be a useful standard for critical information systems where there is a sovereign sensibility. It may even contribute to weaken Europe by making it difficult to express requirements for sovereign hosting and operation when they are needed.

On the contrary a European standard protecting against extraterritorial interferences would also contribute to the development of the European ecosystem of cloud providers.

5.2.2 IT products and services

The European Common Criteria-based cybersecurity certification scheme (EUCC), enacted at the end of January 24 creates a common framework through which IT products can have a recognised cybersecurity certification. It improves on the former mutual recognition of national certifications that was in place.

For the customer, requiring certified products in a call for tender is a clear simplification, at least when there is a corresponding offering.

For the vendor, the cost of making one of its product compliant, and of the certification process itself may be an obstacle. The mutual recognition of certified products that has been in place in the EU, and the newer EUCC, increases the market size for a given certified product or service, and may be enough to make it viable or even a business opportunity. Still, there are many domains where no certified solutions are available, either because of the lake of a specific certification profile, or because no vendor has found it pertinent to create a certified offering.

5.2.3 Networks and communication services

The necessity to address security risks associated with electronic communications has been expressed by the European Union since at least 2009 (Articles 13a and 13b of the Directive 2009/140/EC which lead to the publication of technical guidelines on how to handle them).

Following the adoption of the European Electronic Communication Code (EECC) in 2018, those guidelines have been refreshed by the ENISA (Guideline one Security Measures under the EECC, 4th version, July 2021).

Although interesting for Member States that deploy a state owned network for their administrations, it's only marginally relevant for Tax Administrations, as is the new EU5G certification scheme by the ENISA.

5.2.4 Other initiatives

Several other projects at the European level attempt to provide a place for the consolidation of technical offers, or to facilitate the development or mutualisation of technical solutions, or the mobilisation of data. The most notable ones are:

- GAIA-X which aims at enabling data sovereignty and sharing in the context of clouds, at several levels: sharing infrastructure and services, standardised policies for cloud operators, standardisation of data in specific domains, etc.; it federates or collaborates with several other projects which cater to the same need: AgriGaia, Catena-X, EuroDat, Structura-X,

- The EU Code of Conduct register is a place for cloud and cloud services providers to declare of demonstrate their compliance with GDPR,
- Dome[11], launched on the 4th of July, 2024, want's to create a federated Marketplace for trusted cloud and edge services; from infrastructure and platform as a service, to data, AI, etc. services, including cybersecurity solutions.

Although those initiatives may in the medium to long term lead to new offers or a better way to select technical offers relevant to cyber security, they are still works in progress, and moving quickly mostly when the private actors have identified opportunities (cloud actors of course, as a way to improve their solutions and gain credibility, but also specific actors who would gain from a better environment for sharing data, like the automotive industry or the financial sector).

Those projects clearly have no short to medium term applications for tax administrations as a way to address vendors with regard to digital security and resilience.

5.3 Interesting standards and practices at the country level

5.3.1 Member states standards and certifications

Independently of European standards and initiatives, or specialising in them, Member States have their own bodies of standards, certification systems, projects, etc.

To illustrate:

- Certification systems in France for IT Services specialised in security testing (PASSI), in incident detection (PDIS) and response (PRIS), in administration and maintenance (PAMS), cloud providers (Secnumcloud),
- a specific corpus of standards for administrations in Germany, which addresses most of the aspects of securing information systems, from external cloud services to mobile device management, logging and detection, tls parameters,

No single member state covers all the bases through standards and certification systems for IT products and services.

And when a Member State does not have its own certification framework or standard for a given need, there is real added value in being able to ask the market for a service certified according to the framework of another Member State (for example, for a detection service) or in being able to require compliance with another Member State's standard in its call for tenders (for example, a cryptographic or a logging standard).

5.3.2 Procurement practices

The project found that most of the countries represented had organised procedures and standard security clauses for awarding contracts. It was also found that the standard clauses, and to a lesser extent the procedures, were largely adapted to the national legal framework for procurement and therefore not very reusable or shareable.

This relatively low reusability of practices for procuring IT equipment, solutions and services should not mask the criticality of the procurement process in guaranteeing IT security and resilience and preserving sovereignty.

[11] https://dome-marketplace.eu/

Thus, it may still be interesting that the Member States that have invested most in documenting good procurement practice, share them in a translatable form, even if they will not be directly reusable.

5.3.3 Initiatives with vendors

Several initiatives have been identified that seek to reconcile cloud-based extra-European solutions with the need for European sovereignty:

- Orange, Capgemini and Microsoft have created "Bleu" (Blue), a joint venture that seeks to sell services from the Microsoft portfolio, most notably Office 365 and Azure, in a version located and operated in Europe, and compliant with the French SecNumCloud 3.2 security standard ; the first commercial services are announced for the end of 2024, with a Secnumcloud certification not expected before 2025,
- In a similar scheme, Thales and Google have created a joint venture (S3NS) that is working on instantiating a version of Google cloud services compliant with the Secnumcloud standard.

Some others initiatives have a lower profile but are nonetheless interesting and are helping to develop Europe's sovereign supply of digital and security solutions. That has been the case for cryptographic solutions, advanced detection and responses tools, web services acceleration and protection. Those solutions appear or are promoted at least through:

- certification schemes, where the incentive for a European solution to be certified (giving it first mover status) is higher than for a non-European solution that already has a market abroad,

- call for tenders by administrations were compliance with European standards, or European hosting and operation are required, and more readily doable (and profitable) for European actors.

5.3.4 Open-source alternatives

Open-source solutions (OSS), when they exist to cover a given need and are competitive with closed source / commercial solutions, have a clear edge in terms of control, technological independence, and frequently cost.

The recourse to open-source solutions can be opportunistic, or result from a clear strategy from the Member State or from a given tax administration. For instance:

- France has long been promoting open-source solutions inside administrations which used, contribute to, and even create many them,
- The French tax administration was at the initiative of the first implementation of a large scale software insurance contract covering open-source solutions the place them on the same level as commercially edited ones ; the current implementation of this contract is shared by several administrations and covers more than 300 softwares ; if most of them are server side and not really visible by end users, the tax administration has been using LibreOffice as its office suite since 2010, and has invested significantly in the Samba 4 alternative to Microsoft Active Directory so that it could be robust enough to handle the whole park of workstations (130k) and civil servants (100k) ; Samba AD is now viewed as an asset for control and sovereignty by the French ANSSI and in the course of being evaluated to replace Microsoft AD at the Interior ministry,

- Several German states or municipalities have been long time users of open-source solutions or even have set in place strategies that prioritise open-source solutions; dating back to 2001, Thuringia, North Rhine Westphalia, Baden-Württemberg, Hamburg, and Hesse implemented OsiP to perform security checks for access to airports, nuclear plants, ports, … Munich migrated to OSS in 2003 for its workstations (and back to Microsoft in 2017). Schleswig-Holstein has defined a clear strategy toward open-source since 2012, and is a significant contributor (through Dataport, a multi states owned digital services provider) to the deployment of open-source solutions in states and municipal administrations.

The open-source option is even more relevant when most commercial editors are migrating to cloud based services, even removing from their catalogues the options for on premise or cloudless installation. E.g. while it's working independently on the workstation, the choice of a commercial office suite vs an open-source one is only a question of function and cost ; but when the option of an autonomous, non-sovereign cloud independent office suite disappears from commercial offers, the open-source alternative becomes even more relevant.

This, and other similar needs have been addressed in several Member States:

- In Germany, Dataport has integrated several (many) open-source solutions into Phoenix, a cloud based communication, productivity and collaboration suite, with functionalities ranging from emailing, complete office suite to audio and videoconferencing, chat, group work,
- The German Federal Ministry of the Interior and Home Affairs (BMI), represented by ZenDiS (the Centre for Digital Sovereignty), is attempting to convert Phoenix into a Digital Worplace solution geared to all of European public sector,
- ZenDiS is also managing Open CoDE, a platform to promote the exchange of open-source code between administration and which is part of DVS (the German Cloud Strategy for Administrations),
- In France, similar platforms, integrating most of the same bricks as Phoenix, have been developed both by the private and public sector, two of them being promoted by the French inter-administrations IT directorate for use by administrations,
- Such initiatives would strongly benefit from more collaboration, sharing and reuse between Member States.

5.4 Conclusions and recommendations – Harmonising Standards

The original intention regarding "One voice toward vendors" was both to identify where the participating Tax Administrations were standing in their digital security procurement, the domains where they had specific requirements and, through discussions with "at least four of the biggest IT vendors in Europe", to evaluate the vendors capabilities to deliver to their needs.

The initial working sessions showed that there was a significant difference in approach between the Tax Administrations when it comes to building their information systems, both in terms of the principles and technical choices, and in the range of solutions (and therefore vendors) that can be envisaged (notably because of different sensitivities in terms of sovereignty). There was not going to be a clear set of needs to address with a few vendors.

These sessions also revealed significant differences between countries or TAs in the bodies of standards, clauses and certification processes with which procurement is carried out.

As a result, it was felt that an analysis of existing standards and the needs of participating countries to provide a better framework for their suppliers would be of greater value and a necessary foundation to be able to talk in a coordinated way with vendors in the future.

5.4.1 Key findings

There is a demonstrable interest in addressing the IT and cybersecurity market in a coordinated way:

- to increase leverage on vendors and help obtain solutions that would not emerge or at a much higher cost should they be specified with too much variety,
- ensure that all Tax administrations are equally well equipped to obtain the most relevant and well-defined answers to their needs.
- when addressing the market through a call for tenders, the most pertinent reusable elements mays be common requirements, references to legislations or standards or certification frameworks, generic clauses.
- focusing on what contributes most directly to the continuity of service of an information system, to resilience in the face of the cyber threat, and to the defence of European interests against non-European players:
- the corpus of European legislations regarding cybersecurity and resilience may be pertinent to reference in some call for tenders, but almost never contribute any kind of specification elements of a product or service,
- European standards are slow to appear, especially those regarding cybersecurity and resilience, and only cover a small part of the solutions which are needed (notably, IT services and expertise are not covered); even more, by trying to address the needs and navigate the sensitivities of public and private actors, they risk being irrelevant,
- on the contrary, most of the needs are covered by the combined set of standards, specifications, certification schemes and documented best practices of member countries or tax administrations,
- it's much less true when looked at per country, making it clear that, even if some of those may not be as easily transposed (e.g. procurement clauses which are more dependant of national legislations), there is in most cases a real value in sharing between Tax administrations.

Finally, some needs less central to resilience were also considered for impact on interoperation between tax administrations and sovereignty. The communication tools (audio and videoconferencing) were the first mentioned, followed by office and collaboration tools. For those, the need to identify common or fully interoperable solutions makes it interesting to prospect possible project to build in common or to reuse, either on an open source based or with for adaptations of on the shelf solutions.

5.4.2 Recommendations – Harmonising Standards

Work on existing tools to better address vendors conducted during this project identified both reusable elements at the national or Tax Administration level, and interest from other countries for them.

A more systematic and detailed sharing between interested Tax Administrations is proposed along three lines:

- identification of projects that have a potential for reuse or that could be good candidates for being worked on in common could be done in project groups already in place for sharing on IT projects,
- sharing on standards and certification schemes looks interesting but its effectiveness needs to be asserted ; it is proposed that a temporary group is set up for a period of two years (two to three meetings a year, geared toward Information Security Officers) and if it works that it is transformed into a permanent group,
- similarly sharing of best practices and standard cybersecurity clauses for procurement seems promising ; it is proposed that a specific group addressing those subjects and targeted to Information Security Officers and procurement specialists is set up, once a year, for an experimental period of three years.

6 European collaboration for backup and continuity - enhancing emergency transfer and storage of data between EU Tax and Customs Administrations

6.1 Introduction

In the modern world, Tax and Customs Administrations across European countries must be prepared for emergency situations that could disrupt their operations. Such emergencies might include natural disasters, cyber-attacks, political instability, or any unforeseen events that could jeopardise the integrity and accessibility of critical data. For instance, a significant cyber-attack on a country's Tax and Customs Administrations system could necessitate an immediate transfer of data to another country to ensure continuity of operations and safeguard sensitive information.

This chapter explores how EU Tax and Customs Administrations can collaborate to ensure digital continuity and resilience in the event that one agency becomes inoperable. Specifically, it examines how one Tax and Customs Administrations could practically transfer data to another as part of a continuity plan.

To provide a comprehensive understanding, a fictional scenario has been developed as a case study, evaluating the following key areas:

- The legal feasibility of inter-administration data transfers
- The technical practicality of enabling such transfers and setting up co-location solutions
- The financial implications and potential benefits of these collaborative efforts

The goal is to provide actionable recommendations that enhance data security, operational resilience, and compliance with EU regulations, while ensuring cost-effective solutions for the Tax and Customs Administrations involved.

6.1.1 The Scenario - Background

Two EU Tax and Customs Administrations (TA), TA-A and TA-B, both members of the TADEUS, face the challenge of ensuring digital continuity should one administration's IT systems become compromised. Both administrations manage large volumes of sensitive taxpayer data, and any disruption to their digital infrastructure would negatively impact tax processing, audits, and public services.

To mitigate such risks, TA-A and TA-B have agreed to develop a collaborative data continuity plan. This plan focuses on secure data co-location and the ability to transfer critical systems and data between the two administrations. The partnership ensures that if one administration experiences an outage or cyber-attack, the other can take over core functions to maintain continuity.

6.1.2 The Scenario - The Event

TA-A suffers a severe cyber-attack, resulting in a complete shutdown of its digital infrastructure, including taxpayer databases, digital filing services, and communication platforms. Some backup systems were also compromised, making immediate recovery impossible. To prevent delays in tax processing and avoid financial and reputational damage, TA-A activates its continuity plan and initiates a data transfer to TA-B.

6.1.3 The Scenario - Legal Feasibility

The legal framework for data transfers was established under a bilateral agreement based on EU regulations and data sovereignty laws. Both Tax and Customs Administrations collaborated with national legal advisors and the EDPB to ensure compliance with the GDPR. The agreement stipulates that:

Data will be encrypted both in transit and at rest.

Access to transferred data will be restricted to authorised personnel in TA-B.

TA-B will process only the data necessary to maintain critical services for TA-A.

Data will be returned to TA-A upon system restoration, and any data not immediately returned will be securely deleted or stored.

These measures secure the legal feasibility of inter-administration collaboration without violating data privacy laws.

6.1.4 The Scenario - Technical Feasibility

TA-A and TA-B have invested in creating a secure digital infrastructure that allows for real-time data co-location across multiple EU data centres. Key components include:

Data Co-location: TA-A's data is mirrored in secure, geographically separated EU data centres accessible by both TA-A and TA-B in emergencies.

Encrypted Transfer Protocol: A custom encrypted data transfer protocol compliant with EU cybersecurity regulations ensures secure, automated transfers of taxpayer databases and digital services.

Disaster Recovery Environment: TA-B maintains a disaster recovery setup designed to replicate TA-A's IT systems, ensuring continuity of taxpayer portals and financial reporting services.

Testing and Simulations: Annual continuity simulations validate the integrity and speed of data transfer, ensuring both administrations can seamlessly switch to the backup environment with minimal downtime.

6.1.5 The Scenario - Financial Implications and Benefits

The financial aspects of this collaboration include:

Cost Sharing: By jointly investing in a shared infrastructure, TA-A and TA-B reduce overall costs, avoiding redundant systems.

Avoidance of Private Sector Costs: The use of EU-controlled data centres minimises costs associated with commercial cloud providers while maintaining control over sensitive data.

Minimised Downtime Costs: The rapid transfer of data ensures continuity of tax services, preventing revenue loss and preserving public trust in the tax system.

Enhanced Cybersecurity: Pooling resources enhances both administrations' cybersecurity defences, reducing the risk of future attacks.

6.1.6 The Scenario - Outcome

With the successful activation of the continuity plan, TA-B took over TA-A's core functions during the crisis. Taxpayer services remained operational with minimal disruption. After several weeks, TA-A's systems were restored, and the transferred data was returned securely. Both administrations reviewed the event to improve future collaboration and enhance protocols.

This scenario demonstrates the effectiveness of cross-border collaboration between EU TAs to ensure digital continuity, protect taxpayer data, and maintain public services during emergencies.

6.2 Historic events affecting business continuity in Europe (1990-Present)

Before going into the examination of different possibilities for transferring critical data and maintaining business continuity of affected TAs, here's a brief overview of events that have had a major impact on public services. The events listed below were of such magnitude that disruptions in information flows and data processing were highly likely to occur. Over the past few decades, a number of these incidents have taken place across Europe, affecting public services and, in many cases, revealing vulnerabilities in digital infrastructure and continuity planning. From natural disasters like floods and earthquakes to man-made disruptions such as wars and cyberattacks, these incidents demonstrate the critical importance of resilient digital systems and robust data recovery plans. The experiences drawn from these events have highlighted the need for public entities, including TAs, to adopt advanced business continuity strategies. By examining these cases, we can better understand the risks faced by TAs and the measures required to ensure the secure transfer and storage of critical data across national borders, even during large-scale crises.

6.2.1 Wars and conflicts

Wars and conflicts in Europe have caused direct damage to physical digital infrastructure, including communication networks and data centres:

1999 – Kosovo War: During the NATO airstrikes on Yugoslavia, telecommunications infrastructure was heavily damaged. The bombings disrupted digital communication networks, affecting businesses and government operations in the region. The destruction of physical infrastructure led to significant downtime in IT services.

2014 – Russia-Ukraine Conflict: Russia's annexation of Crimea and the ongoing conflict in Eastern Ukraine caused severe disruptions to digital infrastructure, particularly in the Donbas region. Telecommunication lines, internet services, and data centres were damaged or destroyed, impacting local businesses and government services.

2022 – Russia-Ukraine War: The full-scale Russian invasion of Ukraine targeted critical infrastructure, including power grids, telecom networks, and data centres. Cyberattacks accompanied physical destruction, further crippling Ukraine's digital infrastructure. Ukrainian businesses and public services faced widespread disruptions, forcing the relocation of data and IT services to more secure locations, including within the EU.

6.2.2 Natural disasters

Natural disasters have caused widespread damage to physical IT infrastructure, such as data centres and telecommunication lines, leading to significant service interruptions.

2002 – European Floods: Massive flooding across Central Europe, including Germany, Austria, and the Czech Republic, damaged critical infrastructure such as power grids and

telecommunication systems. Many businesses experienced outages due to the destruction of local data centres and communication lines.

2003 – European Heatwave: The intense heatwave in Europe led to several power outages and failures of cooling systems in data centres, particularly in France and Italy. Overheating equipment caused downtime for businesses relying on these data centres for continuity.

2009 – L'Aquila Earthquake (Italy): The earthquake in Italy caused significant damage to the infrastructure of the affected region, including telecommunication lines and local IT systems. Business continuity was disrupted for companies operating in the area, as physical infrastructure was severely impacted.

2018 – Storm Friederike (Germany and Netherlands): The powerful windstorm caused widespread power outages, disrupting IT systems and telecommunications infrastructure. Data centres and businesses in the affected areas faced downtime due to damage to physical infrastructure.

6.2.3 Cyberattacks

Cyberattacks targeting physical infrastructure have resulted in significant disruptions to digital services and business continuity in Europe:

2015 – Ukrainian Power Grid Cyberattack: Though the attack targeted Ukraine's power grid, it had ripple effects across Europe by highlighting the vulnerabilities of critical infrastructure to cyberattacks. It caused widespread power outages, affecting communication and digital infrastructure within Ukraine and sending shockwaves through European energy and IT sectors.

2021 – Irish Health Service Executive (HSE) Ransomware Attack: A ransomware attack crippled the Irish health service's IT systems, disrupting healthcare services across the country. While this was primarily a cyber-event, the inability to access digital infrastructure led to physical disruptions in healthcare operations, showcasing the importance of resilient digital systems.

6.2.4 Technical failures

Failures in physical infrastructure, including power outages and hardware malfunctions, have disrupted digital operations and caused significant business continuity issues in Europe:

2003 – Italian Blackout: A massive power outage left most of Italy without electricity for nearly a full day. The blackout affected data centres, telecommunications networks, and IT systems across the country, leading to widespread business disruptions.

2006 – European Power Grid Failure: A technical failure in the German power grid caused a cascading outage across several European countries, including France, Spain, and Belgium. The disruption led to widespread telecommunications outages and affected data centres, causing business continuity issues across multiple sectors.

2016 – British Airways IT Failure: A power surge at British Airways' data centre in the UK led to a global IT system failure, grounding flights and causing significant disruptions in airline operations. This event highlighted the vulnerabilities of physical infrastructure (such as power systems) to IT continuity.

2020 – OVH Data Centre Fire (France): A fire broke out at the OVH data centre in Strasbourg, destroying servers and causing major outages for businesses across Europe that relied on OVH's cloud services. Many companies experienced significant downtime and data loss due to the physical destruction of infrastructure.

6.3 Legal considerations

When EU TAs consider transferring and storing critical data across borders, they navigate a multifaceted landscape shaped by legal, regulatory, and operational complexities. Although all EU member states operate under a shared legal framework, including GDPR and other relevant directives, specific challenges arise when handling critical data in different jurisdictions. This section examines the major aspects that TAs must address regarding the transfer and storage of critical data, identifies the associated challenges, and proposes solutions to facilitate compliance and operational efficiency.

6.3.1 Data protection compliance

Data protection compliance is paramount when transferring and storing critical data. While GDPR establishes a robust framework for data protection across EU member states, variations in national interpretations and additional local regulations can complicate compliance efforts. For example, while GDPR mandates stringent requirements for data handling and processing, some countries may impose additional restrictions or requirements that complicate the sharing of critical data.

To effectively navigate these challenges, TAs should establish standardised data-sharing agreements that outline the processes for data handling, consent, and responsibilities of each party involved in the transfer and storage of critical data. These agreements can help clarify the legal basis for data transfers and ensure that all parties are aligned on compliance measures. Furthermore, promoting collaboration among EU TAs to share best practices regarding GDPR compliance will help create a more uniform approach to data protection across member states.

6.3.2 Intergovernmental agreements

Clear intergovernmental agreements are crucial when transferring and storing critical data across EU borders. The absence of such agreements can lead to ambiguities regarding data ownership, liability, and governance, resulting in operational disruptions and legal uncertainties. Additionally, disagreements over data use or responsibilities can hinder collaborative efforts.

To mitigate these risks, TAs should work together to create comprehensive intergovernmental agreements that define the roles and responsibilities of each party concerning data transfer and storage. These agreements should outline governance structures, data-sharing protocols, and conflict resolution mechanisms. Regularly reviewing and updating these agreements is essential to ensure that they remain relevant and adaptable to evolving regulations and operational requirements.

6.3.3 Licensing and operational requirements

The operational landscape for transferring and storing critical data is further complicated by local licensing and regulatory requirements. Different EU countries may impose specific permits or regulatory frameworks that TAs must navigate, depending on the nature of the data being transferred and the services being provided. Understanding and complying with these diverse requirements can present significant challenges.

Establishing a centralised information hub that details licensing requirements and operational regulations for TAs planning to transfer and store data in other EU countries can significantly ease compliance burdens. This hub should provide comprehensive information about local regulatory landscapes and necessary permits, allowing TAs to prepare effectively for cross-border data operations. Additionally, fostering relationships with local regulatory authorities can facilitate smoother licensing processes and provide valuable insights into specific operational requirements.

6.3.4 Data residency and sovereignty

Data residency and sovereignty issues are critical considerations when transferring and storing data in another EU country. Although the GDPR provides a framework for cross-border data transfers, certain countries may have data localisation laws requiring specific data to be stored within their borders. This requirement can complicate data management, especially if TAs rely on centralised data systems that span multiple jurisdictions.

To address these challenges, TAs can utilise cloud service providers that operate data centres in various EU countries to ensure compliance with data localisation requirements while maintaining flexibility in data management. Developing joint policies among EU TAs that address data residency concerns will clarify how critical data will be managed across borders and mitigate concerns regarding data sovereignty.

6.3.5 Dispute resolution mechanisms

Effective dispute resolution mechanisms are crucial when transferring and storing critical data across borders. Jurisdictional conflicts regarding which laws govern operations can complicate the resolution of legal disputes. Furthermore, understanding local legal systems can be challenging, particularly when language barriers or differing legal practices exist.

To address these challenges, TAs should draft contracts that specify the dispute resolution mechanisms to be used, such as arbitration or mediation, to handle conflicts efficiently. Additionally, providing training for personnel on local laws and dispute resolution processes will enhance preparedness and ensure that TAs can navigate legal challenges effectively.

6.4 Technical considerations

When EU TAs engage in transferring and storing critical data, they face numerous technical considerations that must be meticulously addressed to ensure efficiency, security, and compliance. This chapter examines the essential technical aspects related to data transfer and storage, followed by the challenges and preparations necessary for running services in a different IT infrastructure designed to replicate key functions.

6.4.1 Data encryption and security protocols

One of the foremost technical considerations in the transfer and storage of critical data is the implementation of robust encryption and security protocols. As data moves between jurisdictions, the risk of unauthorised access or data breaches increases. Ensuring data is encrypted both in transit and at rest is critical to safeguarding sensitive information.

To enhance security, TAs should adopt strong encryption standards such as with 256-bit keys, which is widely regarded as highly secure. Additionally, implementing secure transport protocols like TLS can protect data during transmission. Regular security audits and assessments are essential to identify potential vulnerabilities in the data transfer processes.

6.4.2 Data integrity and validation

Maintaining data integrity during the transfer process is another crucial technical aspect. Data corruption can occur during transmission due to various factors, including network issues or human error. Therefore, implementing validation checks to ensure that data is not altered or corrupted during transfer is necessary.

Utilising checksums or hash functions (e.g., SHA-256) can help verify the integrity of the data being transferred. TAs should implement automated validation processes that compare the original data with the received data to detect discrepancies and ensure accurate data transmission.

6.4.3 Network infrastructure and bandwidth

The efficiency of data transfer is significantly influenced by the underlying network infrastructure and bandwidth. TAs must ensure that their network capabilities can handle large volumes of data without causing delays or interruptions. Insufficient bandwidth can lead to bottlenecks, hampering the timely transfer of critical data.

To address this, TAs should conduct a thorough assessment of their existing network infrastructure to determine its capacity for data transfer. Upgrading network hardware, increasing bandwidth, or utilising dedicated data transfer channels can improve performance. Implementing data transfer optimisation techniques, such as compression or parallel processing, can also enhance the efficiency of data transfers.

6.4.4 Data storage solutions

Choosing appropriate data storage solutions is vital for effectively managing transferred critical data. TAs need to evaluate various storage options, including cloud storage, on-premises solutions, or hybrid models, considering factors such as scalability, security, and accessibility.

Cloud storage can offer flexibility and scalability, but TAs must ensure compliance with data residency and security requirements. If using cloud providers, TAs should prioritise those with data centres located within the EU to meet GDPR requirements. On the other hand, on-premises solutions may provide greater control over data security but require significant investment in infrastructure and maintenance.

6.5 Technical considerations for maintaining business continuity

Transferring data from one TA to another may initially appear to be a simple task; however, maintaining business continuity during such a transfer presents a significantly more complex set of challenges. While the act of moving data may involve straightforward technical procedures, the practical value of simply transferring data is quite limited if it is not updated in real-time. Outdated information can quickly become obsolete, undermining the accuracy and reliability of the services that depend on it. This limitation emphasises that TAs require a running digital infrastructure not just to store data, but to provide critical services effectively. Operational continuity entails ensuring that these services remain functional and accessible during the transition, which involves implementing backup systems, maintaining interoperability between different IT infrastructures, and preparing for potential disruptions that may arise. Therefore, achieving business continuity is a multifaceted endeavour that necessitates comprehensive strategies to keep critical services running smoothly, highlighting the stark contrast between a mere data transfer and the robust framework needed for sustained operational resilience.

Once critical data has been transferred and stored, the focus shifts to the technical aspects associated with running services utilising this data in a different IT infrastructure. This transition requires careful preparation and consideration to ensure that the necessary functions can be replicated efficiently and securely.

6.5.1 Infrastructure compatibility and configuration

To operate services effectively in a different IT infrastructure, TAs must first assess the compatibility of their existing systems with the new environment. This includes evaluating hardware specifications, software dependencies, and network configurations. The challenge lies in ensuring that the new infrastructure can support the same operational requirements and functionalities as the original setup.

To facilitate this process, TAs should conduct a comprehensive analysis of their current IT landscape, identifying critical components that need replication. Utilising virtualisation technologies can also aid in creating an environment that closely mirrors the existing infrastructure, enabling smoother transitions and minimising disruptions.

6.5.2 Data migration and synchronisation

Data migration is a critical step in establishing services in a new IT environment. It is essential to ensure that all relevant data is accurately transferred and remains synchronised between the old and new systems. This process poses challenges, such as maintaining data consistency and minimising downtime during migration.

TAs should develop a robust migration plan that includes detailed steps for data extraction, transformation, and loading. Implementing automated migration tools can streamline this process, while real-time synchronisation mechanisms can help maintain consistency between the two environments. Testing the migration process in a sandbox environment prior to full implementation can also mitigate risks.

6.5.3 Security and compliance considerations

Operating in a different IT infrastructure requires TAs to re-evaluate their security measures and compliance protocols. The new environment may introduce different risks and vulnerabilities that need to be addressed to safeguard sensitive data and meet regulatory requirements.

To ensure security, TAs should conduct a thorough risk assessment of the new infrastructure, identifying potential threats and vulnerabilities. Implementing layered security measures, such as firewalls, intrusion detection systems, and regular security audits, is essential. Furthermore, ongoing compliance with GDPR and other relevant regulations must be assured by maintaining proper documentation and conducting regular audits.

6.5.4 Staff training and change management

Transitioning to a new IT infrastructure often requires a shift in operations and processes. Staff must be adequately trained to adapt to the new environment, which can present a significant challenge. A lack of familiarity with new systems can lead to inefficiencies and errors in service delivery.

To address this, TAs should implement comprehensive training programs that equip staff with the necessary skills to operate in the new infrastructure effectively. Change management strategies should also be employed to facilitate the transition, including clear communication of changes, support resources, and continuous feedback mechanisms to address concerns and improve operations.

6.6 Financial considerations

The transfer and storage of critical data between EU TAs involves a range of financial costs that need to be carefully managed. Below are the key financial considerations.

6.6.1 Infrastructure setup costs

Setting up the infrastructure required for data transfer and storage is a significant financial burden. This includes purchasing hardware like servers, networking equipment, and storage systems. These initial CapEx can be high, especially if existing facilities cannot accommodate additional demands.

To mitigate these costs, TAs should evaluate the potential to share infrastructure, make use of EU-level data centres, or adopt virtualisation and cloud solutions where feasible. This reduces the need for large physical investments.

6.6.2 Software and licensing costs

Software tools for managing data transfer, storage, encryption, and database administration are essential, but licensing fees can be substantial. These costs increase when large volumes of data are involved, as well as in cases where specialised software is needed to ensure compliance with EU regulations like GDPR.

TAs can reduce licensing costs by negotiating collective agreements for multiple administrations, or exploring open-source software options, provided security and compliance are maintained.

6.6.3 Operational costs

The ongoing costs of running the data storage infrastructure, such as energy, cooling, and IT personnel salaries, must also be factored in. Co-location or shared data centres can increase operational efficiency, but maintaining 24/7 uptime remains expensive.

Energy-efficient data centres and automation of routine processes can reduce these operational costs. Additionally, employing predictive maintenance techniques can prevent costly breakdowns and disruptions.

6.6.4 Data transfer costs

Large-scale data transfers, especially when done across borders or in real-time, incur significant network and bandwidth costs. The frequency and volume of data transferred can quickly drive up expenses, especially when secure, encrypted transfers are required.

Using data compression techniques, scheduling transfers during off-peak hours, and optimising network usage are essential to keeping these costs in check. Where possible, TAs should utilise EU networks or broadband initiatives to reduce cross-border data transfer fees.

6.6.5 Data security and compliance costs

Ensuring the security of sensitive taxpayer data during transfer and storage is crucial, especially in compliance with GDPR. This involves investing in encryption, firewalls, and continuous monitoring systems. High-level security measures are expensive but non-negotiable due to the critical nature of tax data.

A shared, centralised approach to security—where several TAs use the same services—can reduce costs while ensuring compliance. Regular security audits and investments in cybersecurity insurance can also help mitigate potential risks.

6.6.6 Backup and redundancy costs

Data must be backed up regularly to ensure continuity in case of system failures or data loss. Maintaining redundant systems—whether physical or cloud-based—adds to the cost, particularly for real-time data replication and rapid disaster recovery solutions.

To minimise expenses, TAs should adopt tiered backup strategies, where the most critical data is stored on high-speed, secure systems, and less critical data is stored on cheaper, slower-access systems. Incremental backups can also help save on storage space.

6.6.7 Training and personnel costs

The transfer and storage of critical data require specialised personnel trained in cybersecurity, compliance, and data management. Hiring, training, and retaining this expertise come with ongoing financial costs.

TAs can reduce personnel costs by sharing training programs across multiple administrations, using online platforms for continuous learning, and standardising processes to minimise duplication of work.

6.6.8 Contingency and risk management costs

Unexpected incidents, such as data breaches or operational failures, can result in significant financial liabilities. These include legal costs, fines, and expenses related to system repairs and recovery efforts.

Allocating a budget for contingencies is critical, as is investing in cybersecurity insurance to cover potential breaches. Establishing strong incident response protocols can also help mitigate the financial impact of unexpected events.

6.7 Solutions and concepts

When discussing data transfer, storage, and maintaining business continuity between two EU TAs, various solutions and concepts come into play. These strategies must account for legal, technical, and operational aspects to ensure both secure data handling and uninterrupted service provision. Below are the possible solutions and concepts for achieving these objectives:

6.7.1 Data co-location and replication

One of the most effective solutions is data co-location, where critical data is continuously replicated between two geographically separate data centres, both within the EU. Co-location ensures that in the event of a system failure or disaster in one TA (e.g., a cyberattack or natural disaster), the other TA can immediately access the mirrored data and take over operations.

Concept: Real-time data replication is essential to keep both TAs' data fully synchronised. This can be achieved through automated processes that mirror the databases, applications, and configurations in multiple locations. This ensures that no data is lost, and service interruptions are minimised.

Benefits: The data is always available in a secondary location, reducing recovery times in case of failure. It also allows both TAs to be operational, regardless of what happens to the primary infrastructure.

6.7.2 Hybrid cloud solutions

A hybrid cloud model offers a flexible and scalable solution for data storage and business continuity. This model combines on-premises data storage for sensitive information (such as taxpayer data) with cloud-based infrastructure for non-sensitive services.

Concept: By using a hybrid approach, TAs can securely store critical data in EU-based data centres (for GDPR compliance), while leveraging the cloud for computing power and service delivery during emergencies. For example, if a TA’s primary infrastructure fails, its non-sensitive services can quickly shift to cloud environments, enabling it to continue operations.

Benefits: The hybrid cloud provides scalability and cost-effectiveness, while still maintaining control over sensitive data. It also enables fast scaling during high-demand periods (e.g., during tax season), reducing the risk of service downtime.

6.7.3 Disaster recovery as a service (DRaaS)

DRaaS is a cloud-based solution that enables TAs to replicate and host their data and IT infrastructure on a secondary cloud platform, allowing rapid recovery after an incident.

Concept: DRaaS ensures that all critical systems, including applications, databases, and configurations, are replicated in real time to a secure cloud environment. In case of a disaster, the impacted TA can switch to the cloud-hosted environment to continue running essential services such as tax filings and financial audits.

Benefits: This solution guarantees minimal downtime and automatic failover in emergencies. DRaaS is highly scalable and cost-effective, as TAs only pay for the cloud resources they use during regular operations and emergencies.

6.7.4 Interoperable disaster recovery environments

To maintain business continuity, it is essential to ensure that each TA can run the services of the other. This requires establishing interoperable disaster recovery environments that replicate the infrastructure, software, and applications used by the primary TA.

Concept: TA-B would host an interoperable IT environment that mirrors TA-A's infrastructure. In the event of a failure at TA-A, TA-B can take over its critical services, such as taxpayer portals and financial reporting systems. To ensure seamless transition, both TAs need to harmonise their systems and data formats, ensuring smooth interoperability.

Benefits: This approach ensures that services remain operational even if one TA experiences a major failure. It also provides an additional layer of security and redundancy by enabling mutual backup capabilities.

6.7.5 Automated failover systems

An automated failover system is critical for ensuring that services automatically switch to a secondary site if the primary infrastructure fails. This system continuously monitors the health of both TAs' IT environments and triggers an automatic shift to the backup environment if an issue is detected.

Concept: This solution monitors the IT infrastructure for any disruptions or failures. In the event of a cyberattack, hardware malfunction, or other disasters, the automated system instantly switches to the secondary TA's infrastructure without manual intervention.

Benefits: Automated failover significantly reduces downtime, ensuring that services such as taxpayer submissions and audits are uninterrupted. It also minimises the risk of human error in the recovery process, providing a more reliable continuity solution.

6.7.6 Encrypted data transfer protocols

For secure and compliant data transfers between TAs, robust encrypted data transfer protocols must be in place. This ensures that any data transferred between two TAs is protected from unauthorised access during transmission.

Concept: Using end-to-end encryption, such as AES-256, guarantees that data is secure while being transferred between two locations. The data is encrypted before it leaves the originating TA and only decrypted once it reaches the receiving TA, ensuring data integrity and privacy.

Benefits: This protects sensitive taxpayer data during transfers and ensures compliance with GDPR and other data privacy regulations. Secure transfers are crucial during emergency data handovers or continuity processes, particularly when personal and financial information is involved.

6.7.7 Data validation and integrity mechanisms

Maintaining the integrity of data during transfer is critical. Data validation and integrity mechanisms ensure that the data transferred between TAs remains accurate and uncorrupted throughout the process.

Concept: Checksum algorithms (such as SHA-256) and validation processes are employed to compare the original and transferred data. Automated checks detect discrepancies or corruption in the transferred data, allowing for immediate correction.

Benefits: These mechanisms ensure that the transferred data is accurate and that no errors or data corruption occur during the transmission. This is vital for ensuring that taxpayer records and financial data remain intact during emergency transfers.

6.7.8 Incremental and real-time backups

To prevent data loss and ensure that services remain up to date, incremental and real-time backups are essential for both TAs. Incremental backups capture changes to the data at regular intervals, while real-time backups allow instant synchronisation between the primary and secondary sites.

Concept: Incremental backups store only the changes made since the last backup, while real-time backups replicate data as it is created or updated. Both methods ensure that data is continuously updated and preserved in case of a disaster.

Benefits: This approach minimises data loss and recovery time, allowing both TAs to access the latest data during emergency handovers. It also reduces storage costs, as only the changes, rather than full backups, are saved regularly.

6.7.9 Shared EU data centres

Using shared EU data centres provides a cost-efficient and secure solution for storing and replicating data between TAs. These data centres are operated within the EU, ensuring compliance with GDPR and data sovereignty laws.

Concept: Both TAs can store their critical data in a shared data centre located within the EU. In the event of a failure at one TA, the other can instantly access the mirrored data from the shared infrastructure to maintain continuity.

Benefits: Shared data centres offer cost savings by reducing the need for each TA to maintain separate backup infrastructure. Additionally, they provide the security and compliance needed for handling sensitive taxpayer data.

6.7.10 Continuity testing and simulations

Regular continuity testing and simulations are vital for ensuring that all the systems and protocols for data transfer and service continuity work as intended. These tests allow TAs to identify

weaknesses in their disaster recovery strategies and improve upon them before a real emergency occurs.

Concept: Annual simulations involving a full test of data transfer, failover, and recovery processes ensure readiness. Both TAs should simulate disaster scenarios like cyberattacks or power outages to evaluate their resilience and adjust protocols accordingly.

Benefits: Testing ensures that the data transfer and recovery systems are reliable and effective. It also helps improve response times and minimises disruption during actual emergencies.

6.8 Conclusions and recommendations – Co-location

The primary objective of this chapter was to explore how one tax administration could practically transfer data to another tax administration as part of a continuity plan, with consideration given to the results of FPG 126. As part of this effort, a small case study was developed to examine three key areas: a. Legal possibility, b. Technical possibility, and c. Benefits and finance. We thoroughly explored these aspects, identifying the legal framework necessary for secure data transfers, assessing the technical infrastructure required to facilitate such transfers, and evaluating the financial and operational benefits of collaboration between EU tax administrations.

It will not be possible for this group to provide a cost comparison or exact cost amount to enable this solution. Therefore each TA needs to understand its core services, will need to make a BIA, this will let them understand their recovery time objective, recovery point objective, maximum tolerable period of disruption. They will also need to consider among other things; data volume, replication frequency, infrastructure, bandwidth and network, vendor/service provider.

Having addressed these areas, we now turn to the recommendations and proposed solutions that follow from this analysis. These recommendations provide actionable steps for ensuring secure, efficient, and compliant data transfers, while also maintaining business continuity during emergencies.

6.8.1 Optimal solution strategy

The most effective approach for ensuring the secure transfer, storage of data, and business continuity between two EU TAs involves a combination of real-time data co-location, hybrid cloud solutions, and automated failover systems. This strategy is ideal because it provides the necessary flexibility, security, and scalability to ensure that taxpayer data is always protected and that critical services remain uninterrupted, even in times of emergency. Let's break down why this solution is the best, as well as some of its potential downsides.

Why this solution is optimal:

Real-Time Data Co-Location ensures that critical data from both TAs is continuously mirrored in a secure off-site location. This approach reduces the risk of data loss because the data is always available in a secondary location. Should one administration's infrastructure fail, the other can immediately access the mirrored data to maintain services. This is particularly effective because it provides near-instant recovery, minimising the impact of disasters such as cyberattacks or natural disasters.

Hybrid Cloud Solutions offer both flexibility and cost-effectiveness. By using a mix of on-premises storage for sensitive data (e.g., taxpayer financial records) and cloud-based solutions for less critical services, TAs can achieve the best of both worlds. The cloud infrastructure allows for rapid scaling and deployment of services during emergencies, while sensitive data remains

securely controlled in EU-based data centres. This approach ensures compliance with GDPR and data sovereignty laws, while allowing the flexibility to expand services quickly when needed.

Automated Failover Systems provide an immediate response to any system failure. By constantly monitoring the health of the IT infrastructure, these systems can automatically shift operations from one TA's infrastructure to the other without manual intervention. This is a critical advantage because it reduces human error, speeds up recovery times, and ensures that essential public services (like tax filings and audits) continue without significant delays. The automation of this process makes it highly reliable and quick, which is essential during large-scale system disruptions.

Potential downsides:

Cost of Implementation: Real-time data replication, hybrid cloud solutions, and automated failover systems require a significant upfront investment in both infrastructure and technology. Building the necessary data centres, integrating cloud services, and establishing automated systems can be expensive. Smaller TAs with limited budgets might find this difficult to implement without shared resources or external funding.

Complexity: Implementing such an integrated system is technically challenging. It requires close collaboration between the TAs, IT staff with expertise in cloud services, data replication, and cybersecurity. This complexity increases the operational overhead and may necessitate extensive staff training to ensure smooth execution.

Ongoing Maintenance: While cloud-based services can reduce some operational burdens, maintaining automated failover systems and real-time backups can be resource-intensive. Regular testing, upgrades, and cybersecurity updates are necessary to keep the system secure and efficient, adding long-term costs for both TAs.

Data Sovereignty Concerns with Cloud Solutions: Even though the cloud portion of the hybrid solution can be based in EU-compliant data centres, there may still be security concerns for some TAs over having taxpayer data in the cloud, even if it is limited to non-sensitive data. This may be a concern for TAs that deal with particularly sensitive tax information or have strict national regulations regarding data residency.

6.8.2 Recommendation for establishing mutual trust and political will

Before any transfer or storage of sensitive data between two EU TAs can be considered, it is essential to first establish mutual trust and political will as a strong foundation for collaboration. Without this, any technical or legal infrastructure built for data transfer and storage will be on shaky ground. The following recommendations can help foster the necessary trust and political alignment between TAs:

- Create a framework for open dialogue and communication. Why it's important: Trust is built through open, transparent communication. Both TAs must engage in frequent and structured dialogue about their objectives, concerns, and expectations regarding data sharing and collaboration.

  Recommendation: Establish a bilateral working group or task force with representatives from both TAs. This group would meet regularly to discuss the technical, legal, and operational aspects of potential data transfers. These meetings should focus on aligning both parties' priorities, addressing concerns (especially around data privacy), and setting clear expectations for how the partnership would work. Clear communication fosters transparency and helps to build trust over time.

- Develop and sign memoranda of understanding (MoU). Why it's important: An MoU formalises the commitment between TAs and outlines the principles of cooperation, ensuring both parties are aligned and accountable.

  Recommendation: Before formal data-sharing agreements, create a MoU that outlines the general principles of collaboration, including a shared commitment to security, data protection, and compliance with EU regulations such as GDPR. The MoU should define the scope of the relationship, the intentions of both administrations, and the willingness to work together toward shared goals. By signing such a document, both administrations demonstrate their political will to cooperate.

- Engage in joint pilot projects. Why it's important: Pilots help build confidence by demonstrating that collaboration is feasible, beneficial, and aligned with both parties' interests.

  Recommendation: Start with small-scale joint pilot projects that do not involve sensitive taxpayer data but require similar levels of cooperation and technical integration (e.g., sharing non-sensitive data analytics or best practices on auditing systems). These pilot projects will allow both TAs to gradually build trust through successful collaboration, setting the stage for more complex data-sharing arrangements in the future.

- Demonstrate commitment to data security and sovereignty. Why it's important: Both TAs must feel confident that the other is taking data protection as seriously as they are. Any perception of weak security practices will undermine trust.

  Recommendation: Each TA should publicly commit to high standards of data security by adopting best-in-class practices for encryption, cybersecurity, and compliance with EU laws. Sharing details of security policies and GDPR compliance measures builds trust by assuring the other party that sensitive data will be handled with the utmost care. Additionally, both TAs should demonstrate their commitment to respecting data sovereignty, ensuring that data remains under the control of the originating administration, and can only be accessed or used for agreed-upon purposes.

- Leverage EU institutions as neutral facilitators. Why it's important: Involving an impartial third party, such as an EU body, can help ensure transparency and fair dealings.

  Recommendation: Engage EU-level institutions like the European Commission or EDPB to act as neutral facilitators in the process. They can help mediate discussions, ensure that both TAs comply with EU-wide standards, and provide external accountability. This third-party involvement strengthens political will by providing a framework that both administrations must adhere to, minimising the risk of unilateral decisions or mistrust.

- Conduct regular trust-building workshops. Why it's important: Beyond formal meetings, creating informal spaces for dialogue fosters relationships at both the operational and leadership levels.

  Recommendation: Organise joint trust-building workshops and seminars that focus on data security, cybersecurity best practices, and disaster recovery strategies. These workshops allow IT staff, legal teams, and decision-makers from both TAs to collaborate in informal settings, sharing expertise and building relationships. Trust is built not only through formal agreements but also through personal relationships and understanding.

- Align strategic objectives at the policy level. Why it's important: Political will comes from the top. Both administrations need to ensure that their leadership is aligned on the importance of collaboration and the shared benefits of data-sharing.

Recommendation: Engage high-level policymakers and political leaders to emphasise the strategic importance of collaboration. Framing the data-sharing initiative as a shared goal that enhances resilience, operational efficiency, and EU-wide tax administration cooperation helps secure political buy-in. Both TAs should highlight how collaboration will serve broader EU goals, such as enhanced cybersecurity, improved tax enforcement, and resilience against crises.

- Conduct joint risk assessments. Why it's important: Trust is often undermined by fear of the unknown. Jointly identifying risks helps both administrations feel confident in the solutions put in place.

  Recommendation: Before considering data sharing, both TAs should conduct joint risk assessments of potential threats (e.g., cybersecurity risks, legal liabilities, operational failures). This process encourages mutual understanding of vulnerabilities and reinforces the idea that both administrations will work together to mitigate risks. Transparency about risk builds trust, as both parties are made aware of potential issues and committed to addressing them.

6.8.3 Recommendation for intra-administration self-assessment

Before proceeding with the establishment of mechanisms for the practical transfer and storage of data to another TA as part of a continuity plan, it is crucial for each TA to conduct a thorough self-assessment. This self-assessment will allow the administration to determine its readiness, willingness, and capability to engage in such data-sharing initiatives. Specifically, this process should help each TA clarify which data is appropriate for transfer, and whether the necessary technical and operational frameworks are in place to support secure and compliant data exchange.

The self-assessment should cover several key areas, including:

- Willingness to participate in cross-administration data transfers, particularly in regard to sensitive taxpayer data.
- Data classification, focusing on identifying which types of data are suitable for transfer and which must remain within national borders due to legal or security constraints.
- Technical preparedness, assessing the robustness of the TA's current IT infrastructure, cybersecurity protocols, and interoperability with potential partner administrations.
- Operational capacity, evaluating whether the TA has the necessary resources, staff expertise, and procedures in place to manage the demands of real-time data transfers and continuity of services during an emergency.

To facilitate this process, it is recommended that each TA complete an intra-administration self-assessment questionnaire, which has been designed to guide administrations through these critical considerations. The draft questionnaire is included as an Appendix 1 to this report, providing a structured approach for TAs to evaluate their readiness and identify any gaps that need to be addressed before entering into formal agreements with other TAs for data transfer and storage.

This self-assessment is an essential step in ensuring that all participating TAs are aligned in their objectives, technically equipped, and fully prepared for the complexities involved in cross-border data transfers as part of a continuity plan.

7 Education and Awareness Raising

The approach to IT security education across EU Member States varies significantly. However, it is essential to provide security professionals with comprehensive and up-to-date training on IT security matters. Disseminating this knowledge throughout the EU, particularly within the Tax and Customs Administration, is crucial as cyber threats evolve rapidly. Ensuring that training programs are accessible to all Member States is key to maintaining high security standards.

Before going into the topics of Education and Awareness Raising, one has to understand what's meant by the two terms. Education extends beyond university lectures; it also encompasses ongoing professional development within organisations. Employees need to stay informed about the latest security standards, and training opportunities must be actively promoted to enable swift and effective responses to cyberattacks. Raising awareness in this specialised field is equally important. Employees, students, and the public must be reminded that cyber threats are an ever-present and, with the advancement of internet technologies, IT security is increasingly critical.

7.1 Introduction

In an increasingly digital world, the demand for skilled cybersecurity professionals is at an all-time high. Cybersecurity education has become crucial as both public and private sectors face an ever-growing threat landscape. Tax Administrations in particular are prime targets for cybercriminal elements due to the sensitive financial and personal data they handle. These threats range from data breaches and ransomware attacks (see chapter 2.4) to sophisticated fraud schemes, all aimed at exploiting vulnerabilities in tax systems.

Recognising this critical need, educational institutions across the EU have been actively developing and offering specialised programs in cybersecurity. This review aims to assess the current landscape of university courses in cybersecurity across EU member states. By examining the availability, nature and distribution of these educational programs, the review provides insights into how the EU is preparing its future workforce to tackle the evolving challenges in cybersecurity.

7.2 Education

7.2.1 Review of Cybersecurity Courses in EU Member States

This analysis is based on a sample study conducted in multiple member states, offering a comprehensive view of the cybersecurity education offerings within the region. The findings highlight key aspects such as the abundance of Bachelor's and Master's degree programs, the availability of full and part-time study options and the geographical spread of these courses to ensure accessibility. Additionally, the review notes that these programs are predominantly offered by technical institutes, indicating a specialised focus on the technical aspects of cybersecurity education. Efforts by the European Union Agency for Cybersecurity (ENISA) in mapping and promoting cybersecurity courses further underscore the importance of this educational domain.

By equipping future professionals with robust cybersecurity knowledge and skills, the EU aims to fortify its defences against the persistent and evolving threats posed by cybercriminals, particularly in critical sectors like tax administration.

The objective of this review is to assess the landscape of university courses in Cybersecurity across the member states of the European Union (EU). This analysis aims to provide insights into the availability, nature, and distribution of Cybersecurity educational programs within the EU, based on information collected from a sample study conducted across multiple member states.

This is an overview of university courses:

- Full Course is where the focus is solely on the discipline of Digital Security.
- Module is where the part of the course is Digital Security but it is not necessarily the main focus, e.g. Computer Science

Ireland

No of Institutions	**20**
Total no of courses	**73**
Full Course	**46**
Certificate	9
Diploma	2
Degree	21
Masters	14
Module	**27**
Certificate	3
Diploma	7
Degree	10
Masters	7

Germany

No of Institutions	**8**
Total no of courses	**44**
Full Course	**5**
Degree	2
Masters	3
Module	**39**
Degree	17
Masters	22

Italy

No of Institutions	**24**
Total no of courses	**39**
Full Course	**39**
Certificate	10
Diploma	24
Degree	5

Slovenia

No of Institutions	**8**
Total no of courses	**19**
Full Course	**3**
Diploma	2
Masters	1
Module	**16**
Degree	7
Masters	9

Greece

No of Institutions	**10**
Total no of courses	**22**
Full Course	**2**
Diploma	0
Masters	2
Module	**20**
Degree	10
Masters	10

Cyprus

No of Institutions	**6**
Total no of courses	**12**
Full Course	**2**
Degree	
Masters	2
Module	**10**
Degree	6
Masters	4

Sweden

No of Institutions	**24**
Total no of courses	**39**
Full Course	**39**
Certificate	10
Diploma	24
Degree	5

France

No of Institutions	**27**
Total no of courses	**78**
Initial Courses	**63**
3-4 year Licence	63
Continuous Courses	**15**
5 year Masters	7
8 year Doctorate	8

The review of university courses in cybersecurity across EU member states reveals a well-established and diverse educational landscape. The findings indicate a significant presence of both Bachelor's and Master's degree programs in cybersecurity, reflecting the EU's commitment to developing a skilled workforce capable of addressing the complex challenges in this field. These programmes are available in both full-time and part-time formats, catering to a wide range of student needs and schedules and are geographically distributed within member states to enhance accessibility.

- *Abundance of Bachelor's and Master's Degrees*: Across the EU member states, there is a notable presence of both Bachelor's and Master's degree programs in Cybersecurity.
- *Full and Part-Time Options*: These courses are offered in various formats, including full-time and part-time options, catering to diverse student needs and schedules.
- *Geographical Spread:* The courses exhibit a geographical spread within each member state, ensuring accessibility to students across different regions.
- *Offered by Technical Institutes*: Predominantly, the Cybersecurity courses are provided by technical institutes rather than larger, more established universities, indicating a specialised focus on technical aspects of cybersecurity education.

A notable observation is that the majority of these courses are provided by technical institutes, suggesting a focused approach to the technical aspects of cybersecurity education. This specialisation is crucial in equipping Tax Administration IT Security personnel with the practical skills and knowledge necessary to combat cyber threats effectively. Furthermore ENISA plays a vital role in this educational domain by offering resources and maintaining an interactive website that details available courses, although there is room for improvement in keeping this information updated.

7.2.2 Certification

To become a cybersecurity specialist, you need to go through some education programmes and gain a certificate. The EU Member states therefore have different certified

The European Cybersecurity Skills Framework (ECSF)[12] provides an open tool to build a common understanding of the cybersecurity professional role profiles in Europe and common mappings with the appropriate skills and competences required.

The ECSF summarises the cybersecurity-related roles into 12 profiles, which are individually analysed into the details of their corresponding responsibilities, skills, synergies and interdependencies. It provides a common understanding of the relevant roles, competencies, skills and knowledge mostly required in cybersecurity, facilitates recognition of cybersecurity skills, and supports the design of cybersecurity-related training programs.

Popular security certifications for 2024:[13]

- CompTIA Security+
- EC-Council Certified Ethical Hacker (CEH)
- ISC2 Certified Information Systems Security Professional (CISSP)
- ISACA Certified Information Security Manager (CISM)
- ISACA Certified Information Systems Auditor (CISA)

7.2.3 In-house education – the French example

The French tax administration has its own training institute, which runs several schools throughout the country. One of these schools trains the agency's IT specialists, including modules on security in development and operations. The schools for non-IT specialists include awareness-raising modules in their curricula. Specialised information security modules for IT specialists are also offered by the ministry's (separate) school. However, at the time, there is no cursus for training cyber specialists in the finance ministry or tax administration. These courses are only given by the national cyber agency.

7.3 Awareness Raising

Organisations can establish a robust defence against the increasing array of cyber threats by implementing programmes to raise awareness. This not only enhances security awareness and practices, but also might lead to better teamwork throughout the organisation. The European tax and customs administrations includes a variety of different programmes in the scope of awareness raising; IT-security specialists, Security Champions and also Ethical hackers.

7.3.1 IT-security specialists – The German Example

In Germany there are three different types of IT security officers: the information security officer, the project information security officer and last but not least the administrative IT security officer.[14]

Information security is commonly neglected, leaving it behind in day-to-day business. A result often is, if the division of responsibilities is unclear, there is a risk that information security basically becomes "other people's problem." Avoiding this, a main contact person for all

[12] https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

[13] https://www.coursera.org/articles/popular-cybersecurity-certifications
https://www.infosecinstitute.com/resources/professional-development/7-top-security-certifications-you-should-have/
https://www.forbes.com/advisor/education/certifications/best-cybersecurity-certifications/
https://cybermagazine.com/articles/top-10-cybersecurity-certifications-for-businesses

[14] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1002.pdf?__blob=publicationFile&v=1

aspects of information security, an IT security officer, is appointed in every German administration to coordinate the "information security" task within the institution.

The role of the person responsible for information security depends on the type and orientation of the institution called differently. Common titles are IT security officer or IT-SiBe, Chief for short, also known as Security Officer (CSO), Chief Information Security Officer (CISO) or Information Security Manager. The title "safety officer," on the other hand, is often used to describe the people who are responsible for occupational safety, operational safety or plant security.

In order to successfully plan, implement and maintain a security process, you must clearly define responsibilities. Besides that, people must be named who are qualified and who have sufficient resources available to fill this role.

Area information security officer

The German federal customs administration has one area information security officer.

In large organisations, it may be necessary to appoint an IT security officer in the different departments. The area IT security officer is responsible for all security issues relating to business processes, applications and IT systems in his area (e.g. department or branch office). Depending on the size of the area to be looked after, the task of an area IT security officer should be taken over by a person who already has similar experience, e.g. being the area IT representative. It is important to ensure that he or she knows the tasks, circumstances and work processes in the area or department and to be supervised well. An institution's various business processes, applications and IT systems often have various security requirements that may be included in specific security guidelines are summarised and require different security measures. He or she has the obligation to report to the recipient if necessary. They coordinate and interface with the specialist management and external, e.g. participation of external consultants in the matters of IT-security.

They also ensure the implementation of security concepts in the respective department and are responsible for creating and updating safety documentation within the area of responsibility. Finally, the area information security officer supports and coordinates the creation of the IT security concept.

Project information security officer

There's also the so-called project information security officer. They have the same task, with the difference that these are project-specific instead of IT system-specific tasks. The first step would be to implement an IT security officer, if it's required. The officer has to make sure there are safety guidelines in the project and that IT system-specific information are summarised and passed along to the IT security officer. This task includes serving as a contact person for employees on site. Any security-related incidents that may occur during the project need to be reported to the IT security office in an official report.

A project information security officer requires detailed IT knowledge, as this facilitates discussions with employees on site and at the find security measures for the specific IT systems that are useful, as well as project management skills needed to organise user surveys and creation.

In fact, this position only has a temporary responsibility for the processes within the project and organises, coordinates and reports within the project with reference to the security

requirements and the baseline protection methodology of the federal office for information security.

Administrative IT security

At last, we have a special department which is responsible for the administrative IT security. The department harmonises overarching subject areas of IT security and confidential information with the requirements of the individual IT procedures.

It combines tasks of working in the IT security management team and working in the security operation centre and has the competence centre for complex information security and confidentiality-relevant needs of specialist processes and IT procedures as well as for the topic of confidential and the home security-relevant needs of specialist processes and IT procedures as well as for the topic of confidentiality.

The administrative IT security participates in the IT security management team and in the Security Operation Centre.

Conclusion

The responsibility for IT security is not only within one office, it's more like a system of checks and balances. Every IT security officer (project/ administrative) has to report back to the main IT security office, but for their department or project, it's their responsibility that there are guidelines and they are being followed. So the responsibility is separated. This also means, that the German administration or the different institutions not only need one or two IT security specialist, but several. This results in more staff, but also more know-how in this area which leads to a more profound cyber security programme.

7.3.2 Security Champions

Security Champions is an awareness programme for employees used by some European Tax Administrations including the Cypriot and Swedish Tax Administrations IT-department. A Security Champion Program deployed within the organisation and populated by ordinary IT staff is a cost-effective solution by leveraging existing personnel to bolster the agency's security defences.

Security champions can disseminate information about the latest threats, phishing scams, and data protection measures, reducing the likelihood of security breaches resulting from human error.

In today's fast-changing digital world, cybersecurity is a big concern for everyone in an organisation, not just the IT department. To deal with the constant threats, it is essential to make security everyone's responsibility. This is where Security Champions step in, helping connect the security team with the rest of the employees. Security Champions are regular employees from different departments who take on extra duties to promote and enforce security practices. They act as a bridge between the security team and their colleagues, making sure everyone understands and follows security guidelines. They are not full-time security experts, but passionate about cybersecurity and get special training to stay updated on the latest threats and protections.

The main job of a Security Champion is to create a security-aware culture in their team. They are the first to spot potential security risks and weaknesses in their department. They also promote safe habits like using strong passwords, updating software regularly and careful internet use. Additionally, Security Champions act as a link between the security team and other employees, making sure everyone understands security policies and incidents clearly.

The Swedish example

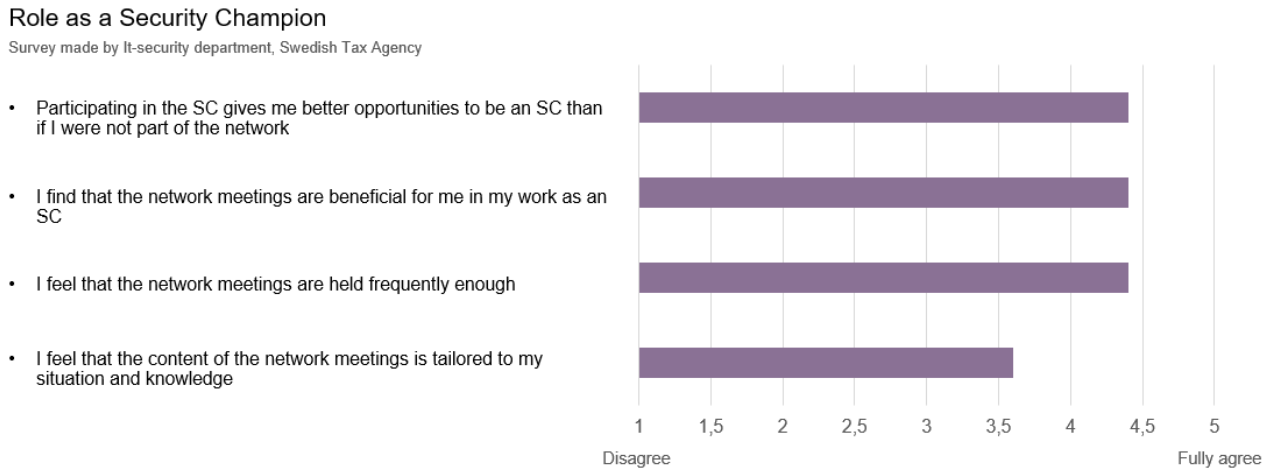
The Swedish Tax Agency handles vast amounts of sensitive taxpayer information, making them prime targets for cyberattacks. The agency decided in 2023 to establish a Security Champion Programme within the IT department. With Security Champions embedded throughout different SAFE of the Agency, it can detect and respond to cyber threats more rapidly. These champions serve as frontline defenders, promptly identifying suspicious activities or anomalies in data access patterns. By reporting incidents promptly and following established protocols, they can help mitigate the impact of cyberattacks, such as data breaches or ransomware infections, minimising disruption to agency operations and safeguarding taxpayer information.

The frequency of Security Champion meetings can vary depending on factors such as the size and complexity of the organisation, the maturity of the security programme and the specific goals of the Security Champion Programme. However, a common approach is to have Security Champions meet regularly, such as once a month or once every two weeks. Regular meetings help ensure that Security Champions stay informed about relevant security issues, updates, and initiatives within the organisation. These meetings also provide an opportunity for Security Champions to discuss challenges, share best practices and collaborate on security-related projects.

Additionally, it is essential to maintain open lines of communication between Security Champions and other stakeholders such as security teams, development teams and management. This can help ensure that security concerns are addressed in a timely manner and that security initiatives are aligned with the organisations overall goals and priorities.

A Security Champion Programme deployed within the Swedish Tax Agency and populated by ordinary IT staff proved to be a cost-effective solution. Instead of hiring additional cybersecurity specialists, the agency empowered internal employees as security champions, providing them with the necessary training and support to fulfil their roles effectively. The Security Champions conduct continuous education. Education ensures they have the knowledge necessary to identify risks, implement security measures and respond appropriately to security incidents. The Swedish Tax Agency has received more attention towards security related questions since the implementation of the Security Champion Programme.

A survey made by the Swedish Tax Agency's IT security department among the Security Champions showed the following results:



According to the survey Security Champions find they have a crucial part in identifying and resolving security issues effectively across the organisation. They are dedicated to their

responsibilities, taking proactive steps to promote best practices and foster a culture of security awareness among their peers. By actively engaging with colleagues and sharing their knowledge, Security Champions contribute significantly to strengthening the overall security posture of the agency. Their commitment ensures that all team members remain informed and vigilant, thereby reducing risks and enhancing the agency's resilience against potential threats.

The Cypriot example

The Cyprus Tax Department introduced the Security Champions programme as part of a project targeting in strengthening the department's information and IT security. Within this context the Security Champion role was added in the organisation's structure, drafted a set of responsibilities, prepared suitable training methods and material and selected Security Champions among colleagues.

Security Champions maintain a constant communication with the organisation's Information Security Officer and the Data Protection Officer. They are scattered throughout the organisation's physical locations and promoting information security awareness, influencing the organisation's culture and act as a first line of support.

Security Champions responsibilities may include but not limited to the following points:

- Ensure the compliance with the Information Security and Data Privacy policies, procedures and processes.
- Support the Information Security Officer and Data Protection Officer in the implementation of location specific initiatives.
- Provide recommendations to enhance information security or data privacy
- Capture and report any information security and data privacy incidents and issues for immediate remedial action.
- Provide support to the organisation's staff in relation to any day-to-day information security and data privacy matters.
- Provide security awareness trainings to the local office.
- Participate in Business Continuity (BCP) and Disaster Recovery (DRP) scenarios and activities.

The initial champions training included an in-depth security awareness training and a "train the trainers" sessions. Starting by providing a set of pilot information security awareness trainings, to the organisation's employees. They offered a controlled environment and a real-life experience of practicing their knowledge and skills. Of course, Security Champion's training has to be on a continuous basis.

The two main challenges of introducing and maintaining the role of Security Champion in our organisation are: selecting suitable people for this task and providing continuous training and updates.

Conclusions

Security Champions have an essential role in enhancing an organisation's cybersecurity defences. By leveraging knowledgeable and proactive individuals across different departments, organisations can establish a robust defence against the increasing array of cyber threats.

Implementing a Security Champion Programme not only enhances security awareness and practices, but also cultivates a culture of teamwork and vigilance throughout the organisation.

It is vital to ensure that Security Champions receive ongoing training to stay current with evolving cybersecurity threats and best practices. They serve as the frontline support for employees on matters related to information security and data privacy. Dedicated training material tailored to their roles are essential to equip them with the necessary knowledge and skills to effectively fulfil their responsibilities. This continuous investment in training reinforces their ability to identify and mitigate risks promptly, thereby bolstering the overall resilience of the organisation against potential cyber threats.

In addition to having a Security Champion Programme and other security-related policies and routines, it is also recommended to take advice from ENISA or the European Union Agency for Cybersecurity, which is an organisation within the EU focused on bolstering digital security measures across member states. It offers expertise and aid to EU nations in strengthening their defences against cyber threats. ENISA fosters collaboration among EU member states, international organisations, industry stakeholders and academia to assess cybersecurity risks, develop policies, and share best practices. Additionally it supports capacity-building initiatives to enhance cybersecurity skills, provides guidance on standards and practices and offers assistance during cyber incidents by providing technical expertise and coordination support. Ultimately ENISA's efforts aim to strengthen digital security across the European Union and ensure the resilience of its digital infrastructure and economy.

Applying policies and procedures, monitoring and communicating information security issues in large organisations is challenging. Aspects like geographical distance among the various locations and handling important and sensitive information like tax data make the situation even more difficult and demanding. A convenient and efficient solution to these issues is the use of champions, a group of trained employees scattered throughout the organisation's buildings.

The Security Champion program involves choosing people in your organisation to promote good security practices. This process can come with its own challenges and successes. Experiences can be really useful the Swedish and Cypriot Tax Administration are happy to share their experiences so far in the implementation of a security champion program. The Swedish and Cypriot Tax Administration can share tips on how to pick and train champions, how to get the whole team involved, and how to deal with any resistance. Talking about both what went well and what was difficult can give a clearer picture of what to expect.

7.3.3 Ethical Hacking

The reason why we emphasise on ethical hacking in this report, is because our attention was caught by an example followed by the Hungarian Government and described to us by a member of our group. These two examples briefly highlight how training and setting up a team could look like.

The French example

The French tax administration has its own internal auditing, penetration testing team. This team also operates as a red team to contribute to the training of the incident detection and response team. It's constituted of former network engineers, system administrators and developers that were trained to become pen testers. When this team was created, around 2008, the training was provided by a contractor which was immersed in the team and stayed for several years. Since then the training has mostly been done by experimented team members (with the addition of some short external formations). The main challenge is keeping the

experts in this team on the long term, and having their expertise recognised although there professional career is not following the standards of a tax administration employee.

The Hungarian example:

In Hungary, the government has taken proactive steps to bolster its cybersecurity defences by establishing a specialised Ethical Hacking Team within the National Tax and Customs Administration (NAV). This initiative is part of a broader strategy to address and mitigate the increasing threats posed by cyberattacks to governmental systems and sensitive data.

In order to become a Certified Ethical Hacker for the Hungarian National Tax and Customs Administration, one has to go through a two-year program, where learning hours take place on Fridays (after 12 midday) and Saturdays (morning to afternoon). It involves theoretical and strong hands-on preparation while being a member of a Cross-Functional Team. Final examination is a two-week procedure with theoretical and practical challenges and tests.

7.3.4 Security Awareness Training

Humans are an integral part of the workflow of every tax administration and in many cases is also considered to be the weakest link in terms of security. A security awareness program can be considered an effective tool to overcome this weakness.

By regularly informing and educating the workforce, a strong barrier against cyber-attacks can be created as well as protecting the information owned by the tax administration. Security awareness programs can be provided through a number of methods. Below follows a description of three of the most common methods of delivering them.

- Physical training can be used as part of the employee's orientation process with physical interaction, where questions from the participants can be answered and discussed during these sessions. It will provide a solid basis for any future training. These initial security awareness trainings may also include material dedicated or customised to the organisation, for example, policies, procedures, GDPR and NIS regulations.
- Web and internal portals are a convenient solution for regularly informing and updating employees and contractors with related material. Relevant products are readily available as a third-party solution and can be used with minimal effort. Providing security awareness programmes via web and internal portals allows to easily monitor the attendance of the participants and also obtain a feedback on participant's maturity level and material assimilation through tests.
- Interactive applications can be similar or part of the web and internal portals approach. Providing interactive material, such as a game, provides an easy-to-understand exercise in a more cheerful manner. An example of such a game is the AR-IN-A-BOX package provided by the ENISA which can be downloaded through their webpage (see next chapter).

An organisation can use one or more methods to inform and train its workforce. With each way having advantages and disadvantages, the organisation can choose the method(s) to implement a security awareness program based on its needs and requirement.

Another important aspect of the security awareness training material is the ability to catch the participant's attention. This a common challenge when presenting technical material or matters. Finding ways to bypass this issue might be as simple as:

- Using examples of the tax administration's everyday life.

- Share and comment on results from real tests performed in the organisation (vishing, phishing).
- Keep the duration of the training as short as possible.
- Use micro-learning as a way to provide memorable pieces of information.
- Provide cases of how security matters are similarly important in participant's personal life with every day examples (strong passwords, spams on personal email, frauds related to obtaining money).
- Indicate the personal responsibility of the participants to information security.

7.3.5 Security Awareness – The ENISA example: AR-IN-A-BOX

ENISA is an EU agency that supports EU cyber policy, enhances the trustworthiness of ICT products, services and processes, and helps Europe prepare for the cyber challenges. The agency has developed a range of tools to support public sector organisations within the area of awareness, albeit not solely for tax and customs administrations.

"Awareness raising in a box" for instance is a programme that has already been developed by ENISA and is a comprehensive solution designed to meet the needs of public bodies, operators of essential services, and both large and small private companies. It provides theoretical and practical knowledge on how to design and implement cybersecurity awareness programmes and is free and available for all TADEUS members today.

AR-IN-A-BOX (Awareness training in a box) is a comprehensive solution for cybersecurity awareness activities designed to meet the needs of public bodies and both large and small private companies. It provides theoretical and practical knowledge on how to design and implement effective cybersecurity awareness programmes with the goal of achieving change of cybersecurity culture. In order to get a glimpse of the hands-on content presented in this tool, there is the possibility to enrol in an online game, using the EU-Login account entering the EU-academy.[15]

This game is designed to evaluate participants' cybersecurity awareness level against common cyber threats.

Players engage in solving a riddle by answering questions related to cybersecurity. Through this interactive approach, participants are encouraged to apply theoretical knowledge to practical scenarios, thereby reinforcing their understanding of cybersecurity principles. The game serves as a self-assessment tool to gauge one's cyber awareness and contribute to achieving a higher common level of cybersecurity across Europe.

It includes guidelines and instructions on/for:

- *building* custom awareness programmes for internal use within an organisation.
- *creating* targeted awareness campaigns for external stakeholders.
- *selecting* the appropriate tools and channels to effectively reach the target audience.
- *developing* Key Performance Indicators to evaluate the effectiveness of a programme or campaign.

[15] https://academy.europa.eu/courses/ar-in-a-box-game

- the development of a *communication strategy*, crucial for achieving awareness objectives.
- the development of internal and external cyber *crisis communication* plans.

It also includes an awareness raising quiz to test comprehension and retention of key information and a game provided in different versions and styles along with a guide on how to play.

The scope of this educational package could be described as followed:

- *Educational Settings*: AR-in-a-Box is designed for use in schools, universities, and training centres. It serves as an immersive tool for teaching complex subjects by bringing theoretical concepts to life.
- *Professional Training*: It can be used in professional environments for training purposes, such as in medical, engineering, and technical fields, where practical, hands-on experience is critical.
- *Corporate Training and Development*: Companies can use AR-in-a-Box for employee on boarding, skills development, and safety training, providing interactive and engaging learning experiences.
- *Marketing and Product Demos*: Businesses can use it for product demonstrations and marketing campaigns to showcase products in an interactive and engaging manner.
- *Research and Development*: It can be a valuable tool for researchers and developers in fields such human-computer interaction (HCI), facilitating the development and testing of new applications and technologies by providing statistics and data-visualisation drawn from real-world scenarios.

The expected results, outcomes and advantages of AR-in-a-BOX are the following:

- *Enhanced Learning Experience:* AR-in-a-Box provides an immersive and interactive way to learn, making complex and abstract concepts easier to understand and retain.
- *Engagement and Motivation:* The interactive nature of AR-in-a-Box captures users' attention and keeps them engaged, which can improve motivation and participation in learning activities.
- *Practical Application:* It allows for the practical application of knowledge in a controlled, risk-free environment, which is particularly beneficial in fields requiring hands-on practice.
- *Customisation and Scalability:* The platform can be customised to fit various educational and training needs and can be scaled to accommodate different group sizes and learning environments.
- *Cost-Effective Training:* By simulating real-world scenarios and providing virtual hands-on experiences, AR-in-a-Box can reduce the need for physical materials and resources, making training more cost-effective.
- *Immediate Feedback:* Users can receive immediate feedback on their performance, helping them to understand and correct mistakes in real-time.

AR-in-a-Box offers a versatile and powerful tool for enhancing education and training across various domains, making learning more engaging, effective, and accessible.

7.4 Conclusions - Education and Awareness Raising

The evolving landscape of digital threats necessitates that tax and customs administrations across the EU adopt robust cybersecurity measures. As these institutions handle sensitive financial and personal data, they are prime targets for cyberattacks. This chapter, about Education and Awareness raising, outlines various strategies and programs developed to enhance IT security within these critical government sectors, highlighting the importance of education, awareness-raising, and specialised roles in building resilience against such threats.

Education is a cornerstone in building an effective cybersecurity workforce. EU member states have taken significant steps to develop specialised programs in cybersecurity across universities, particularly focusing on the technical aspects needed to address cyber threats. Bachelor's and Master's degree programs in cybersecurity are increasingly available, with technical institutes leading these efforts. These programs aim to equip future professionals with the skills necessary to fortify tax administrations against increasingly sophisticated cyber threats.

The European Union Agency for Cybersecurity (ENISA) plays a key role in mapping and promoting these educational programs, while the European Cybersecurity Skills Framework (ECSF) provides a standardised understanding of roles and competencies required in the field. Certifications such as CISSP, CEH, and CISM are recognised across the EU, ensuring that cybersecurity professionals meet high standards of expertise and preparedness.

Beyond formal education, raising awareness within tax administrations is crucial for a holistic security approach. Awareness programs, such as those facilitated by ENISA, are vital in educating employees about the evolving nature of cyber threats. These initiatives ensure that all employees - not just IT staff - are equipped to recognise and respond to cybersecurity risks.

Security Champions programs, adopted by countries like Sweden and Cyprus, involve selecting employees from various departments to act as liaisons between the security team and their colleagues. These individuals receive specialised training and promote security practices, fostering a culture of vigilance and security across the organization. For example, in Sweden's Tax Agency, Security Champions play a pivotal role in rapidly identifying suspicious activities and mitigating risks.

Ethical hackers, also known as white hat hackers, are a critical component in modern cybersecurity strategies. Their role involves identifying vulnerabilities before malicious actors can exploit them. Ethical hacking is institutionalised in several EU member states, including Hungary, where the National Tax and Customs Administration has established a dedicated Ethical Hacking Team. This team simulates cyberattacks on the administration's IT infrastructure, identifying weaknesses and strengthening defences. The program in Hungary provides a two-year, hands-on certification for ethical hackers, emphasising practical skills and teamwork in cybersecurity.

Given that human error is often the weakest link in cybersecurity, awareness-raising campaigns are essential. Security awareness training can be delivered through various methods, including physical workshops, web-based training portals, and interactive tools. ENISA's "Awareness Training in a Box" is a comprehensive program that combines theoretical and practical elements, offering public bodies and private companies resources to design effective cybersecurity awareness campaigns.

In addition, continuous education and reskilling programs for existing staff within tax administrations are recommended. These programs allow employees to switch career paths

towards cybersecurity, providing a fast and efficient way to address the shortage of qualified cybersecurity professionals in the public sector.

The question is: do we need more programmes in the EU member states to raise awareness for Cyber security? The answer is: no. Looking back at the bachelor's and master's programme in the member states, we already have a lot of courses to offer people to educate themselves. Also, the government focuses on putting the spotlight on Cyber resilience and security. The authorities establish more and more IT security specialists such as Security Champions or Ethical hackers.

7.5 Recommendations - Education and Awareness Raising

The recommendation is to utilise existing European programmes on digital security and to start looking at how to reskill the workforce.

Awareness programmes are an important part of all European Tax and Customs Administrations today and are set up to maintain and strengthen the current work force within the field of digital security. General awareness is an essential part of maintaining a healthy digital environment within an administration. A high level of general awareness can help prevent serious breaches of an administrations digital defence. Below are examples of awareness programmes that are free and available today:

- Awareness raising in a box , see chapter 7.2.14
- Security Champions, see chapter 7.2.6-7.2.9

7.5.1 Engage with the Cyber Skills Academy

The Cyber Skills Academy (CSA) builds on four pillars: *Knowledge & Trainings, Stakeholder Involvement, Funding & Projects and Measuring Progress*. The CSA is a way of joining forces on a European level. The CSA is a European policy initiative with its roots in ENISA, aiming to bring together existing initiatives on cyber skills in Europe and improve their coordination. An overriding aim of this initiative is to close the cybersecurity talent gap and boost competitiveness, growth and resilience.[16]

7.5.2 Reskill the existing workforce

Based on the facts that public sector is not very appealing to specialised security professionals and the scarcity of such professions already affecting the public sector all over the EU, a practical and quick solution must be provided.

Take advantage of the education proposals, frameworks and paths mentioned in this chapter and apply them to the existing workforce will provide an effective way out from this difficult situation the public sector is in.

Through organised campaigns the tax administrations can offer, on a voluntary basis, the opportunity to their employees to be reskilled or switch professional orientation. This will provide, at least partially, the resources needed, in a quick and controlled manner, using the existing and readily available human resources.

[16] https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy).

8 Thoughts and suggestions on follow up activities

If the following activities, prioritised, by the project group are of interest of the TADEUS assembly the project group can further develop the chosen activities at a later stage. Looking closer at aspects such as timeframes, expected value and problems solved.

8.1 Create a permanent IT Security Professionals Network group on Digital Security.

The network group would be a forum for IT-security matters related questions and challenges within the tax administrations. It would work with knowledge/information sharing and presentations in relation to items such, as but not limited to;

- General IT Security matters
- Security Standards
- Legislative requirements (e.g. NIS2 implementation)
- Staffing and skills issues
- Propose work stream groups for topics where no knowledge currently exists.

The main reason for creating the group is that there is no permanent specialised Digital Security forum currently within the EU tax and customs administrations.

The network group should consist of IT-security professionals preferably ISOs and/ or Subject Matter Experts (SME). The group would ideally be meeting quarterly with the agenda being focused on specific topics proposed by the participants.

8.2 Preparing for Emergency transfer of data

Would your administration want to be a host? Would you like your administration to ask another administration to transfer its data to you or vice versa?

The group would focus on two items, preferably in order:

- Matchmaking – Identify power, willingness and potential of one administration to host other administrations data, information etc.
- The practical side of preparations – make an initial study in order to evaluate needs and wants. The legal aspects of transferring data between member states. The concrete architectural side of the transfer as the data needs to be accessible as well as safe. Consolidating feedback from pilot projects.

There is a long term rise in threat level, both cyber and otherwise, in Europe. The complexity of carrying out any transfer of data let alone in an emergency, the benefit of being prepared. Making preparations would be lowering the risk in a risk management context.

The group would be working on pilot projects and in working groups. Participants would be on the legal as well as IT-operative level; participation needs initial agreement at strategic level.

8.3 Sharing best security practises in procurement

The group should be sharing best practises in procurement as well as harmonisation and sharing of standards.

Sharing of best security standards will streamline the procurement process and provide a set of baseline security standards.

The target group would be both Information Security Officers (ISO) and procurement specialists.

The group could be either temporary or permanent - experimenting on sharing. It could be as an FPG or just an annual sharing of best practises on minimum security standards for the procurement side of the administrations purchasing. Some subjects can be included in existing groups. This group should be tested during a 2 year period and if it works carry on working otherwise disband.

8.4 Levelling up digital security competence of IT resources

The group would share and create procedures, courses and programmes of how to practically go about upskilling existing IT staff.

Collaborating in this way would be combating the scarcity of Digital Security competence due to the constantly changing landscape of evolving threats.

The group would consist of HR-managers and strategic level IT-managers meeting twice a year.

9 Appendix 1 – Digital Sovereignty – Self Assessment

Appendix 1 Digital sovereignty - Self asse

10 Appendix 2 – Co-location – Self Assessment

Appendix 2.
Co-location Self Asses

List of sources

- Deutsche Bundesbank (2019): "Geldpolitik im Euroraum". https://www.bundesbank.de/de/service/termine/geldpolitik-im-euroraum-kompakt-strategie-und-instrumentarium-des-eurosystems-902914 (last access on 15/12/2022 at 11.13am).
- ATOS: https://atos.net/en/lp/digital-sovereignty-cybersecurity-magazine/what-is-sovereignty-and-why-it-does-matter (last access on 30/07/2024 at 11.09am).
- Agenzia per l'Italia Digitale: https://www.agid.gov.it/
- Dipartemento par la trasformazione digitale: https://innovazione.gov.it/dipartimento/en/structure/
- COMPUTER SECURITY INCIDENT RESPONSE TEAM – ITALIA: https://www.csirt.gov.it/
- ASPERIQ: " LEARNING FROM THE RANSOMWARE ATTACK ON TIETOEVRY'S DATA CENTRE:": https://www.asperiq.com/article/ransomware-attack (last access on 30/07/2024 at 11.09am).
- Wired.com: https://www.wired.com/story/the-us-government-has-a-microsoft-problem/ (last access on 30/07/2024 at 11.25am).
- Myndigheten för Samhällsberedskap(2023): " Erfarenheter från Ukraina -Initiala lärdomar för det civilaförsvaret" https://www.msb.se/contentassets/5d70a3f1096d46348e1ae3acf257689c/fo2023-01325-erfarenheter-fran-ukraina_initiala-lardomar-for-det-civila-forsvaret.pdf (last access on 30/07/2024 at 11.30am).
- ENISA: " Cyber Resilience Act Requirements Standards Mapping - Joint Research Centre & ENISA Joint Analysis) https://www.enisa.europa.eu/publications/cyber-resilience-act-requirements-standards-mapping (last access on 30/07/2024 at 11.31am).
- Dome: https://dome-marketplace.eu/ (last access on 30/07/2024 at 11.35am).
- ENISA: "The European Cybersecurity Skills Framework" (ECSF) https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework (last access on 30/07/2024 at 11.35am).
- Coursera: "10 Popular Cybersecurity Certifications" https://www.coursera.org/articles/popular-cybersecurity-certifications: (last access on 30/07/2024 at 11.40am).
- Infosec: https://www.infosecinstitute.com/resources/professional-development/7-top-security-certifications-you-should-have/ (last access on 30/07/2024 at 11.42am)
- Forbes: https://www.forbes.com/advisor/education/certifications/best-cybersecurity-certifications/ (last access on 30/07/2024 at 11.43am)
- Cyber Magazine; https://cybermagazine.com/articles/top-10-cybersecurity-certifications-for-businesses (last access on 30/07/2024 at 11.45am)
- The Official Website of the European Union: " AR-in-a-Box Game " https://academy.europa.eu/courses/ar-in-a-box-game (last access on 30/07/2024 at 11.46am)
- ENISA: https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-raising-in-a-box (last access on 30/07/2024 at 11.49am)

- The Cyber skills Academy: https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy (last access on 31/07/2024 at 14.56am)
- Bridges, William. Managing Transitions: Making the Most of Change. Cambridge, MA: Da Capo Press, 2009.
- Brown, Jeffrey W. Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers. New York: Fortune, 2015.
- Bygrave, Lee A. Data Privacy Law: An International Perspective. Oxford: Oxford University Press, 2014.
- Carr, Nicholas G. The Big Switch: Rewiring the World, from Edison to Google. New York: W.W. Norton & Company, 2008.
- DiGiovanni, Yvonne. "Best Practices in Data Migration for Business Continuity." Journal of Data Management 23, no. 2 (2018): 152-165.
- European Commission. Interoperability Solutions for Public Administrations (ISA): Guideline on Establishing Interoperability Frameworks. Accessed May 2023. https://ec.europa.eu/isa/actions/03-interoperability.
- Gregory, Peter H. CISSP Guide to Security Essentials. New York: McGraw-Hill, 2012.
- Heiser, Jay, W. Timothy Polk, and Karen Scarfone. "Guidelines on Security and Privacy in Public Cloud Computing." National Institute of Standards and Technology (NIST), 2011. https://nvlpubs.nist.gov.
- Hill, David G. Data Protection: Governance, Risk Management, and Compliance. Boca Raton, FL: CRC Press, 2009.
- Hunter, Richard G. The Real Business of IT: How CIOs Create and Communicate Value. Boston: Harvard Business Review Press, 2009.
- Kaminski, Margot E. "The Right to Explanation, Explained." Berkeley Technology Law Journal 34, no. 1 (2019): 189-220.
- Kavis, Michael J. Architecting the Cloud: Design Decisions for Cloud Computing Service Models (IaaS, PaaS, and SaaS). Hoboken, NJ: Wiley, 2014.
- Kotter, John P. Leading Change. Boston: Harvard Business Review Press, 2012.
- Kuner, Christopher. "Data Protection Law and International Data Transfers: Essential Issues." International Data Privacy Law 3, no. 4 (2013): 230-244.
- Loshin, David. Master Data Management. Burlington, MA: Elsevier, 2009.
- Marks, Eric A., and Bob Lozano. Executive's Guide to Cloud Computing. Hoboken, NJ: John Wiley & Sons, 2010.
- Mather, Tim, Subra Kumaraswamy, and Shahed Latif. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. Sebastopol, CA: O'Reilly Media, 2009.
- Preston, W. Curtis. Backup & Recovery: Inexpensive Backup Solutions for Open Systems. Sebastopol, CA: O'Reilly Media, 2007.
- Reuvid, Jonathan. The Secure Online Business Handbook. London: Kogan Page, 2008.
- Schulz, Greg. Cloud and Virtual Data Storage Networking. Boca Raton, FL: CRC Press, 2011.
- Tanenbaum, Andrew S., and David J. Wetherall. Computer Networks. Boston: Pearson, 2011.
- Tzanou, Maria. The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism. Oxford: Hart Publishing, 2017.

- Voigt, Paul, and Axel von dem Bussche. The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer, 2017.
- Wiewiórowski, Wojciech. "Cross-border Data Flows and GDPR: Impact on International Business." European Data Protection Supervisor (2020). https://edps.europa.eu.
-