The Second Belt and Road Initiative
Tax Administration Cooperation Forum
(BRITACOF)

Topic 4
Tax Related Data Governance

(7-9 September 2021)

Data Security Control

in the Italian Revenue Agency

Paolo Valerio Barbantini
Italian Revenue Agency
(Deputy Director General)

Outline

Introduction

1. Infrastructure security
2. Data Repositories security
3. Access control and logging
4. Security Awareness
5. Conclusions

Introduction: Data Security - the governance framework

The Italian Revenue Agency has adopted a structured set of measures aimed at:

- enforcing **adequate levels of security** and protection of collected data and information; and
- ensuring **data quality**

Governance - General Data Protection Policies

General policies and guidelines - Responsibility model for officers - Awareness of officers and stakeholders

1. Infrastructure security	2. Data repositories security	3. Access control and logging	4. Data quality assurance
Security measures on: • communication channels • Authentication, Authorization and Accounting of senders • Received and transmitted messages	• Authentication and authorization for access - only through applications • Appropriate measures and safeguards to ensure protection of personal data information	• Access limitation for confidential information • Logging of all activities to support awareness and allow following investigations • Alerting	• Measures to improve the quality level of collected information

1. Infrastructure security

Data are exchanged (only) through **secure channels and services**, designed and provided by the Agency

Registration	Permission to send data is granted only after a structured registration and validation process
Sender identification	When exchanging data, digital certificates are used to ensure identity of senders
Channel encryption	Communication channels are protected through channel encryption
Content encryption	Exchanged data are encrypted and digitally signed
Secure Reception systems	Reception systems perform first correctness checks on received data flows and acquire data securely

2. Data Repositories security

- Internal and external “data consumers” (incl. machine-to-machine) are allowed to access data exclusively **through applications** verifying user authentication and authorization
- External entities are allowed to **access data only by specific service agreements** defining scope, terms and conditions, communication channels and restrictions (as well as rules ensuring compliance with privacy requirements)
- **Advanced analysis** of information is allowed exclusively in compliance with internal privacy and security policies

3. Access control and logging

- A rigorous access control policy prevents unauthorized accesses from external users
- Internal unauthorized accesses are tackled by logging sessions

No direct access is allowed. Access to data for officers and external users is allowed **exclusively through applications**.

All accesses are authenticated, and specific user roles define authorizations to read and modify data.

A specific security policy formalizes an **authorization workflow to assign access rights to users**. The workflow is supported by a specific tool.

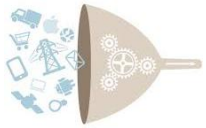
All operations on data are logged for following inquiries. For critical services, a log collector has been implemented to ease control activities.

Focus on access control

Within the new access control system, **a new approach to the resources authentication and authorization access** have been defined - based on a standard, open source and microservice approach

Multifactor authentication

Single login and single sign on



Multiple credentials can be used by users

User

Single logout

Standard, open source and future proof technology

Fully integrated and modular

4. Security Awareness - Targeted communications inside and outside the Agency

In addition to specific technology measures and protection systems, Agenzia delle entrate regularly plans and executes **Security Awareness campaigns and communication activities**, in order to keep high focus on secure behaviors

IT people

- **Web Application Penetration Test (WAPT)** specific training, in order to update skills and enforce processes for in-house developed application
- IT people is anyway Included in Security Awareness employees campaigns

Employees

- During last two years (2020 and 2021), **4 runs of the Security awareness campaign** (including phishing simulation) have been performed (and are in progress, reaching out 19k employees by dec 2021)
- In 2022 **completion of campaign for all 33.000 employees is planned**, together with **cyclic scheduling** of updated campaigns

Citizens

- **Targeted security communication** to citizens and intermediaries, specifically on phishing (Web portal, Twitter, Facebook,), for phishing campaigns and scam domains sharing
- **Dedicated information area** on Agency's web site in order to share out PoV and increase behaviour awareness

5. Conclusions

1. Priority: **strong commitment** for Ade in ensuring Data Security
2. Pre-requisite to ensure **trust and reliability** *vis-a-vis* external stakeholders
3. Need to focus not only on technology but also on awareness and **«cultural» changes** as well
4. Increase in the use of technology needs increased **investments** in resources and skills
5. Not a «one-size-fits all» approach, but an ongoing and **continual improvement** process

The Second Belt and Road Initiative
Tax Administration Cooperation Forum
(BRITACOF)

Topic 4
Tax Related Data Governance

(7-9 September 2021)

Data Security Control

in the Italian Revenue Agency

Paolo Valerio Barbantini
Italian Revenue Agency
(Deputy Director General)