

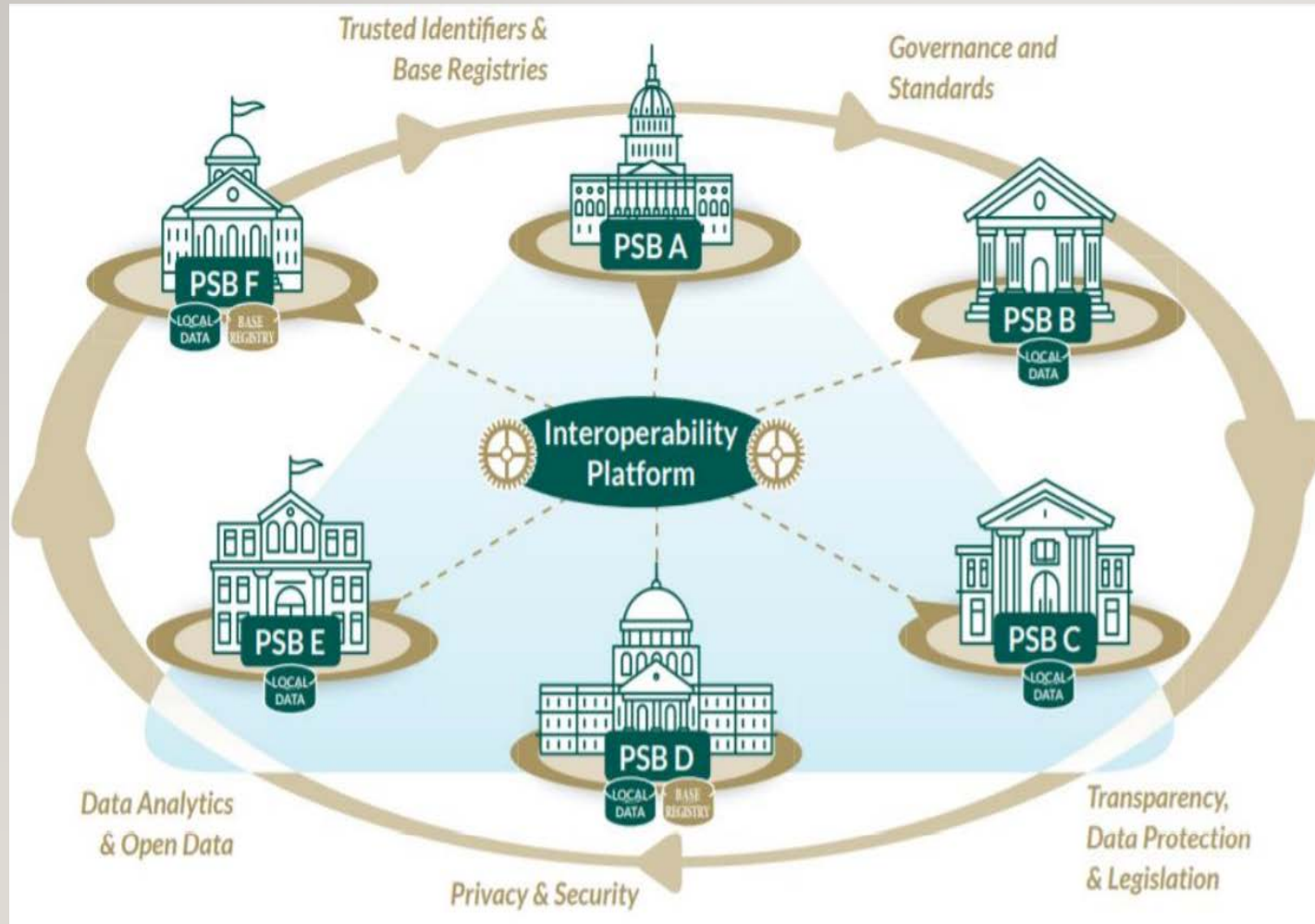


## 2 CONTENTS

---

- Data Protection and Security for Tax Data
- Information Security System
- Key Success Factors

### 3 DATA MANAGEMENT FOR PUBLIC SERVICES



“To establish a data ecosystem that will improve how we govern, manage and re-use data in a secure, efficient, and transparent way, for the benefit of citizens, businesses and policy makers”.

Government of Ireland, Public Service Data Strategy Vision

## 4 TAX DATA

---

- Value of Data:

Tax authorities receive a lot of confidential information from individuals and businesses in a digital format. They also routinely exchange taxpayer information with other governmental bodies. Furthermore, tax administrations have put a lot of work into developing systems for new standards of automatic exchange of information under multilateral or bilateral agreements.

## 5 ETHICAL ISSUES IN USING DATA

---

### **Data Science Ethical Framework of the UK Government:**

- 1-Start with clear user needs and public benefits**
- 2-Use data and tools, which have the minimum intrusion required**
- 3-Create robust data science models**
- 4-Be alert to public perceptions**
- 5-Be as open and accountable as possible**
- 6-Keep data secure**

## 6 DATA PROTECTION

---

Data protection is the process of safeguarding important data from corruption, compromise or loss and providing the capability to restore the data to a functional state should something happen to render the data inaccessible or unusable.

# 7 DATA PROTECTION

---

1-Traditional Data Protection

2-Data Security

3-Data Privacy



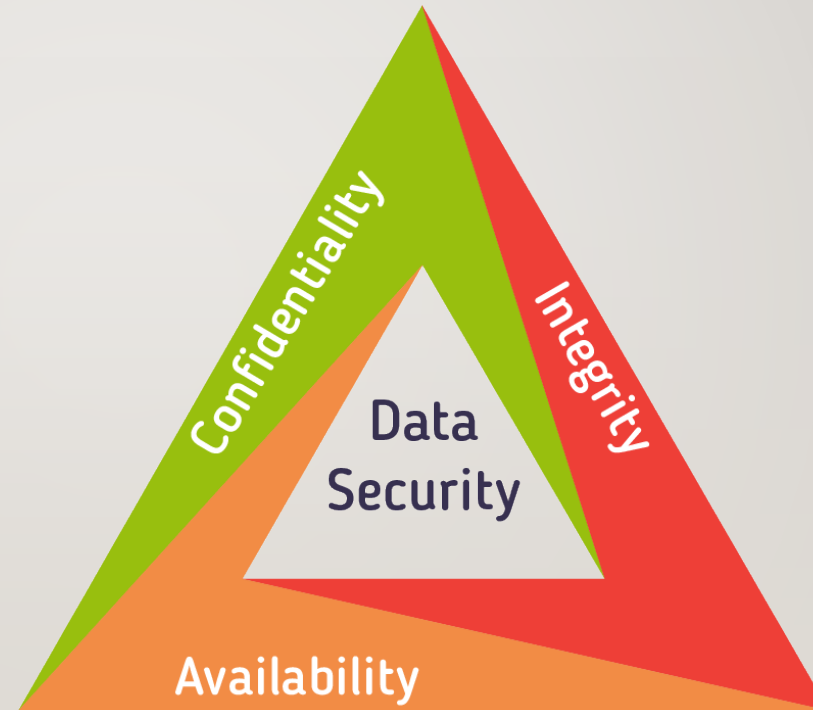
## 8 GOALS OF DATA SECURITY

---

1-Confidentiality

2-Integrity

3-Availability





## 9 **WAYS TO GUARD AGAINST THREATS**

---

- DEVELOP A CYBERSECURITY POLICY BASED ON ESTABLISHED GUIDELINES
- ESTABLISH CYBERSECURITY COUNCIL WITH INDUSTRY AND ACADEMIA
- CREATE A CULTURE OF CYBERSECURITY AWARENESS

# 10 KEY SUCCESS FACTORS IN ESTABLISHING AN INFORMATION SECURITY SYSTEM

---

- Culture
- Technology and Infrastructure
- Skill and Ability
- Management and Support
- Processes

## II CULTURE

---

- Understand the importance of information security
- Existence of a holistic and systematic approach
- Accept the importance of learning and education
- Creating a culture for system acceptance

## 12 TECHNOLOGY AND INFRASTRUCTURE

---

- The state of information and communication technology in the organization
- Existence of computer hardware in the organization
- Employees access to information technologies
- Existence of security policies
- Alignment of information security strategy with the existing information system strategy of the organization

## 13 SKILL AND ABILITY

---

- Employee ability
- Staff knowledge
- Use expert consultants
- Having responsible employees

## 14 MANAGEMENT AND SUPPORT

---

- Manager support for system implementation
- High motivation of the manager to increase the efficiency of the organization
- Organization staff alignment

## 15 PROCESSES

---

- Control and classification of information assets of the organization
- Comprehensive feedback system for performance measurement
- Project risk management
- Operations and Communications Management

## 16 RESULT

---

Privacy laws require organizations to have a proactive approach towards privacy and the protection of personal data. As a result, organisations are enhancing and strengthening the way they handle and govern personal data across its lifecycle i.e. collection, use, transfer, retention, destruction for personal data that belongs to customers, employees, vendors and other stakeholders.



**The END**