Antigua & Barbuda zooms into AEOI

Presented by
Craig Layne

20 February 2025

Tax Administration Performance Summit '25

<u>Antigua & Barbuda’s Experience with AEOI and Global Forum Data Safeguards Assessments</u>

Lessons Learned & Best Practices for Compliance.

Presented by: Craig Layne, IT Manager of the Inland Revenue Department.

Event: *Curacao Tax Administration Performance Summit 2025*

Introduction – Why We Are Here.

- **Why This Presentation?**
  - Sharing **Antigua & Barbuda's AEOI compliance journey** from **2014 to 2025**.
  - Preparing for our **fourth Global Forum Data Safeguards Assessment** and our **third transmission with MDES** in 2025.
- **Why It Matters?**
  - Strong **data protection and security** are critical for **FATCA & CRS compliance**. ISMS Framework, such as **ISO 27000**, formal or informal.
  - **Small tax jurisdictions** face unique challenges in meeting international standards.

Here are the three unique challenges that small tax jurisdictions face:

- Limited IT & Cybersecurity Resources – Small IT teams must handle multiple roles, making implementing and maintaining security controls that meet international standards challenging.
- High Cost of IT Security Compliance – Meeting Global Forum security standards requires significant financial investment in **encryption**, **secure tax systems**, **penetration testing**, **disaster recovery simulation and risk management integration**, which can strain budgets.
- Managing Compliance Across Multiple International Standards – Small jurisdictions must simultaneously comply with **CRS, FATCA, Global Forum safeguards**, and cybersecurity best practices, leading to overlapping and sometimes conflicting requirements.

What is the Global Forum Data Safeguards Assessment?

The Global Forum Data Safeguards Assessment is an evaluation process conducted by the Global Forum on **Transparency and Exchange of Information for Tax Purposes** (OECD Global Forum). It ensures that jurisdictions exchanging taxpayer information under the **Automatic Exchange of Information** (AEOI) framework have strong confidentiality and data protection measures in place.

Key Objectives of the Assessment.

- **Verify Data Security Controls –** Ensuring that taxpayer information exchanged under CRS **(Common Reporting Standard)** and FATCA is protected from unauthorized access, cyber threats, and breaches.
- **Assess Legal & Operational Frameworks –** Evaluating whether jurisdictions have laws, policies, and procedures to maintain data confidentiality and comply with international standards and that these are implemented and measured.
- **Review IT Infrastructure & Risk Management –** Checking whether jurisdictions have secure IT systems, encryption protocols, access controls, and audit mechanisms to protect exchanged data.
- **Ensure Compliance with Global Standards –** Confirming that jurisdictions meet OECD, FATCA, and international cybersecurity requirements for tax data exchange.

Why It Matters.

- A strong safeguards rating ensures continued participation in AEOI, preventing blacklisting or reputational damage and potential de-risking.
- Failing the assessment may lead to restrictions on data exchange, affecting a country's ability to receive critical tax information from other jurisdictions.
- It helps tax authorities strengthen their IT security and legal frameworks and build long-term resilience against cyber threats and data breaches.

The Beginning – Early FATCA Preparations (2014-2015).

- **2014: Initial FATCA preparations began** – Support and guidance from the **Eastern Caribbean Central Bank (ECCB)**. It was determined that the IRDs would be the focal point for the AEOI.
- Discussions were in shared or stand - alone approach to transmission solution.
- **2015: St. Kitts assisted with developing Antigua & Barbuda's policy framework** for AEOI.
- The IRD strengthened collaboration with Central IT in the Ministry of Information to approve policies and frameworks, provide oversight and monitoring.
- Hardening of the IRD was implemented by installing access controls, security cameras, and other security measures. Improve documentation, incident management and escalation.
- **Challenges Faced:**
    - Limited **technical infrastructure** for AEOI.
    - No established **data protection policies**.

Implementing AEOI Infrastructure (2016-2017).

- **2016: Newgen AEOI system was implemented for FATCA filings with the IRS**. (Separate network segmentation, servers, software solution, security certificates etc.

- **2016: IRD enrolled with IRS IDES portal** for secure FATCA transmissions.

- **2016: User Acceptance Testing (UAT) & Training** conducted with **Financial Institutions (FIs)**.

- **2016: Assistance from HMRC, His Majesty's Revenue and Customs** (UK) for FATCA & CRS technical preparations.

- **2017:** AEOI **portal upgraded** to support **both FATCA & CRS filings** from a **single platform**.

Assessments & Evaluations (2016-2019).

- **2016: First Global Forum Confidentiality & Data Safeguards Assessment** conducted.
- **2018: Second Global Forum Assessment** – Identified **gaps in IT security and legislation**.
- **2018: Tax Diamond ICT Assessment** (World Bank) – Analyzed IRD's **IT landscape** for AEOI and the IRD.
- **2019: TADAT (Tax Administration Diagnostic Assessment Tool) assessment** conducted at IRD.

✅ **Key Findings from These Assessments:**

- Need for **stronger encryption & access controls**.
- Gaps in **business continuity & incident response planning**.
- Small IT team **struggled with meeting growing compliance demands**.
- Need for the implementation of a formal **Information Security Management System. ISO 27000 etc.**

Strengthening IT Security & Compliance (2019-2022).

- **2019-2022:** Focused on **enhancing data security, penetration testing, & risk management**.
- **2022: Third Global Forum Assessment** – Major improvements in:
    - **Informal ISO 27001 framework**. Like implementing more restrictive IT security standards through firewalls etc.
    - Proof to support the implementation and monitoring of AEOI policies.
    - **Multi-factor authentication (MFA)** introduced.
    - **Encryption of taxpayer data** fully implemented.
    - **Regular vulnerability scans** conducted.
    - **Updating and expanding the IRD's risk register.**

✅ **Antigua & Barbuda Received Positive Global Forum Feedback**

Transitioning to MDES AEOI System (2023-2024).

- **2023:** Due to **new Global Forum security requirements**, IRD **switched AEOI providers** from **Newgen to BLYCE MDES AEOI**.
- **2023-2024: Successfully completed two transmissions** (FATCA & CRS).
- **Challenges with the transition:**
    - Aggressive timeline for transitioning to the MDES solution.
    - Training **IRD staff** and **Financial Institutions** on the **new platform**. AEIO Unit.
    - Ensuring **data migration security** and compliance with **OECD standards**.
    - **System integration issues** with existing tax infrastructure worked through.
    - Migrating to a cloud-based hosted solution at **Blue NAP Americas**.

✅ **AEOI Transmission Fully Operational with MDES**

Preparing for the Fourth Assessment (2025 & Beyond).

- **Upcoming Global Forum Confidentiality & Data Safeguards Assessment in 2025.**
- **Key Focus Areas for Compliance:**
  - Enhancing **Business Continuity & Disaster Recovery (BCP/DRP)**. IRD and Portals.
  - Expanding **penetration testing & vulnerability scanning frequency**.
  - Strengthening **vendor risk management & third-party IT security**.
  - **Addressing IT resource shortages** with regional collaboration.
  - Implementing **SLA's**, and **SOP's** with Government agencies providing services and support to the IRD.

The Importance of Using Experienced Service Providers

Why Engaging Skilled Cybersecurity Service Providers Matters

- Ensures compliance with international security standards **(OECD, FATCA, CRS).**
- Provides specialized expertise in penetration testing, vulnerability assessments, and IT risk management.
- Helps address technical gaps identified in Global Forum Data Safeguards Assessments.
- Supports small IT teams by offering continuous security monitoring and training.
- Many of these services are not available on island.

Core Security & Compliance Services

✔ **Penetration Testing –** Identifies security vulnerabilities in web applications, networks, and APIs to prevent breaches.

✔ **Vulnerability Assessments –** Conducts regular scans to find weaknesses before hackers do.

✔ **Simulated Phishing Attacks –** Tests staff awareness and trains employees to recognize cyber threats.

✔ **Dark Web OSINT Reviews –** Detects if sensitive tax data has been leaked on the dark web.

✔ **Cybersecurity Awareness Training –** Equips tax authority staff with knowledge on best security practices.

Data Protection & Compliance Services

✔ **Security Policy Development –** Ensures IRD meets Global Forum, NIST, and local cybersecurity laws.

✔ **Continuous IT Security Monitoring –** Provides ongoing threat detection to protect taxpayer data.

✔ **Business Continuity & Disaster Recovery Planning –** Strengthens IRD’s resilience against cyberattacks & system failures.

Benefits of Using Cybersecurity Experts for Global Forum Assessments

How It Strengthens IRD's Compliance & Security Posture

- **Ensures AEOI data security –** Protects sensitive taxpayer information in accordance with OECD guidelines.
- **Reduces IT security risks –** Helps IRD pass penetration testing requirements during assessments.
- **Provides independent security validation –** Demonstrates proactive cybersecurity management to Global Forum reviewers.
- **Supports IT teams with ongoing security improvements –** Ensures sustainable compliance beyond assessments.
- **Builds a culture of cybersecurity awareness –** Trains staff to identify and prevent security threats before they become incidents.

Key Takeaways & Lessons for Other Jurisdictions.

-

- **Start IT security enhancements early**—don't wait for assessment findings.
- **Leverage Regional & International Support**—we benefited from **ECCB, St. Kitts, His Majesty's Revenue & Customs (HMRC), World Bank, IMF**.
- Conduct international assessments like TADAT and Tax Diamond.
- **Regular penetration testing & vulnerability scans** are **critical** for compliance.
- **Managing vendor risks** is key—choosing the right AEOI provider matters.
- **A small IT team can still be effective** with the right **automation & training**.

1. **Improved Risk Register Covering Confidentiality & Information Security Risks**

✔ **Why It's Important:**

- Ensures systematic identification and mitigation of risks in both business operations and IT security.
- Helps track vulnerabilities in data storage, access control, and information exchange.
- Demonstrates proactive risk management to meet OECD Global Forum expectations.

✔ **Key Focus Areas:**

- Classifying IT-related risks **(e.g., cyber threats, unauthorized access, data breaches).**
- Implementing risk mitigation strategies for AEOI data protection.
- Conducting regular updates to keep the risk register aligned with evolving security threats.

Strengthening Internal Audit & IT Policies for Compliance.

1. **Approaches for Internal Audit of the Information Security Framework**

✓ Why It's Important:

- Verifies that security policies & controls are effectively implemented and measured.
- Ensures continuous improvement in data protection and incident response.
- Identifies compliance gaps before Global Forum assessments.

✓ Key Focus Areas:

- Conducting independent security audits on data confidentiality controls.
- Assessing user access management, encryption policies, and IT governance.
- Recommending remediation steps for non-compliant security practices.

IT-Related Policies & Compliance Expectations.

✓ **Why It's Important:**

- Provides a clear framework for handling tax data securely.
- Aligns with **ISO 27001, NIST**, and **OECD** Global Forum requirements.
- Reduces the risk of legal and compliance violations.

✓ **Key Focus Areas:**

- Strengthening data retention & disposal policies to prevent unauthorized data leaks.
- Enforcing password management & multi-factor authentication (MFA).
- Establishing strict access control & audit trails for sensitive tax information.

Final Thoughts & Discussion.

- **How do we keep pace with evolving security threats?**
- **Should regional collaboration be expanded for shared IT security resources?**
- **Final words of advice for those preparing for their first assessment?**

✅ **Q&A Session to Engage the Audience**

Thank You

For your attention