EUROSAI
IT Working Group

# Parallel Audit on Biometric Passports

## Overall results (anonymised)

July 2015

EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE

# Preface

Most of us have a passport, but what exactly lies behind this document?

Advanced technology has brought about the biometric passport, and all such passports must meet the same international requirements. Equal standards indeed – however, data processing, as well as the production and distribution of the passports, happen on a national level. And not just any data... Once fingerprints are widely used as a means of identification, biometric passports grant governments easy access to highly sensitive data in need of being protected accordingly.

For the IT audit specialists of the Supreme Audit Institutions in Europe, this constituted ideal grounds for conducting their first parallel audit. Six nations carried out an audit simultaneously and according to the same audit instructions and programme in a closely defined field. Some exciting results have been obtained, now being presented in the brochure at hand.

The Swiss Federal Audit Office is highly honoured to have been entrusted with the lead in this premier experience. We thank our colleagues from Norway, Portugal, Belgium, Lithuania and Latvia for their confidence and their great contribution to this very fine achievement!

*Swiss Federal Audit Office,*
*Michel Huissoud*



# Table of Contents

# Management Summary

The evaluation of the reported results showed that the overall passport process is generally under control while a couple of high-risk findings were identified in the non-process-specific assessments. In the non-process-specific assessments, most of the countries found deficiencies and weaknesses related to the IS/IT system and the IT management. Medium risks have been identified in the area of laws and regulations, cost-benefit realisation and transparency, as well as in security regulations relating to internal and external personnel.



# Introduction

## Background

As countries have the same duties concerning biometric passport issuance and have to comply with the same ICAO requirements, the execution of a parallel audit of the biometric passport management process seemed sensible.

Therefore, at the 8th Meeting of the EUROSAI IT Working Group (ITWG), held in Paris, France, in 2013, the Swiss Federal Audit Office (SFAO) agreed to take the lead for a Parallel Audit on Biometric Passports to be carried out in 2014.

Having outlined the major aspects relating to the audit project, the SFAO assumed the organisation and coordination as well as the elaboration of the detailed Common Programme for this parallel audit.

The following Supreme Audit Institutions (SAI) confirmed their participation:

- Belgium
- Latvia
- Lithuania
- Norway
- Portugal
- Switzerland

*Note: For confidentiality reasons the sequence of the above-mentioned countries does not reflect the sequence of the results stated below.*

## Subject area

A biometric passport (or ePassport) contains biometric information which serves to authenticate the identity of travellers. Biometric passport management is the process of establishing and implementing the regulation on standards for security features and biometrics in passports and travel documents issued by the member states. The aim is to develop and maintain efficient and secure biometric passport production procedures.

The complexity of the biometric passport process has encouraged many countries to develop (or acquire) computerised information system(s) accompanied by a set of controls. These controls ensure that transactions are recorded accurately and in a timely manner and that transmission channels are secured.

Although member states are bound by the European Regulation on Biometric Passports, there remains the need for national provisions, particularly concerning the issuance procedures and the authority to read and match the data. Moreover, essential questions (e.g. the problem of nation-wide databases) are not addressed by the Regulation and thus left to the member states.

The biometric passport production process includes a combination of software, hardware, people and communication systems that enable and support data input, processing, storage and the issuing of the documents. Biometric passport production is thus dependent on information systems to ensure that states can produce reliable products.

# Objective and scope of the audit

## Audit objective

The objective of the audit was to assess whether adequate management and control processes are in place relating to the biometric passport production process. Within the primary objective, auditors were expected to ascertain whether the process to obtain a reliable and secure biometric passport is well defined and properly implemented.

The main goal of this audit was to validate the following areas with regard to the production process, including the risk mitigation aspect:

- Benefit realisation
- Security
- Effectiveness and efficiency

The central control objectives and questions to clarify were as follows:

- Is IT aligned with the business (i.e. strategic direction for IT provides stakeholder value)?
- Does IT enable the business and maximise benefits (cost optimisation, innovation, risk reduction)?
- Are IT resources used securely and responsibly?
- Are IT-related risks managed appropriately?

## Key risk areas

The key risk areas include but are not limited to:

- Loss/theft of physical assets and/or electronic information
- Misuse of confidential information
- Non-cost-effective process and procedures (financial risk)
- Reputation risk
- Compliance risk (failing to meet legal and regulatory requirements)
- Sourcing risk

Each participating country was free to decide how the audit should be performed and what exact audit criteria and methods from the Common Audit Programme should be applied.

## Audit scope

The scope of the Parallel Audit on Biometric Passports was to review the full process of application, creation and distribution of the passports, and the storage of confidential data. On a high level, the audit was divided into 'Passport process assessment' and 'Non-process-specific assessment'. While the first part focused more on the process itself, the second part covered the underlying requirements (e.g. information systems/technology/management, laws and regulation, cost benefit and personnel).

The review of specific data privacy requirements and adherence to technical biometric security standards were not covered by the scope of the Parallel Audit on Biometric Passports.

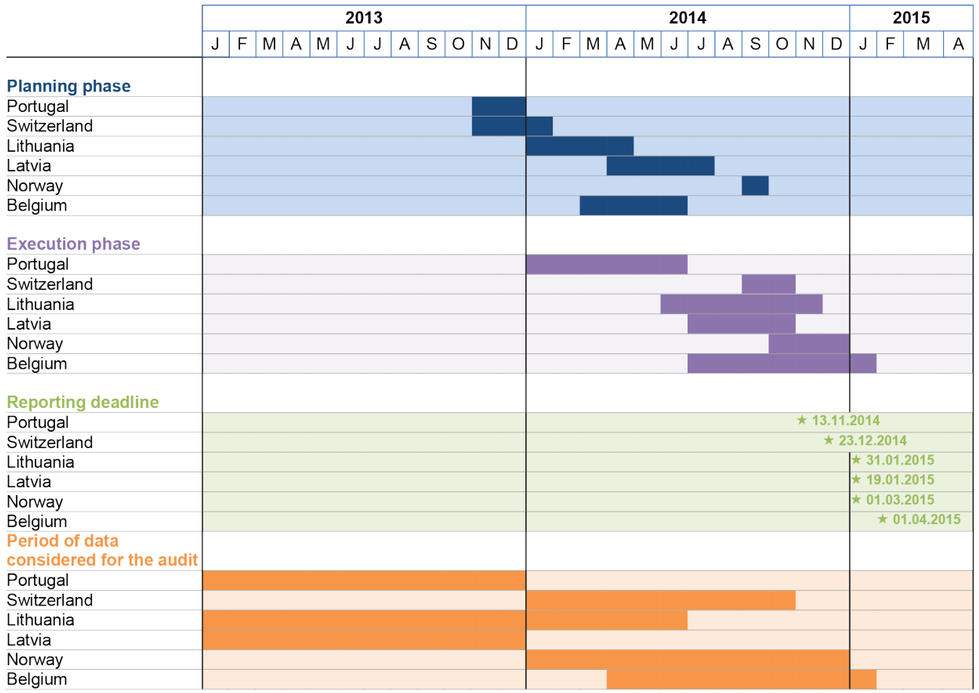
Based on discussions during a workshop held in Paris, the decision was taken to perform this audit according to the COBIT 4.1 framework, where applicable. Furthermore, the following underlying frameworks were used to design the Common Audit Programme:

- ISO 27002
- ICAO - International Civil Aviation Organization (Doc. 2909)

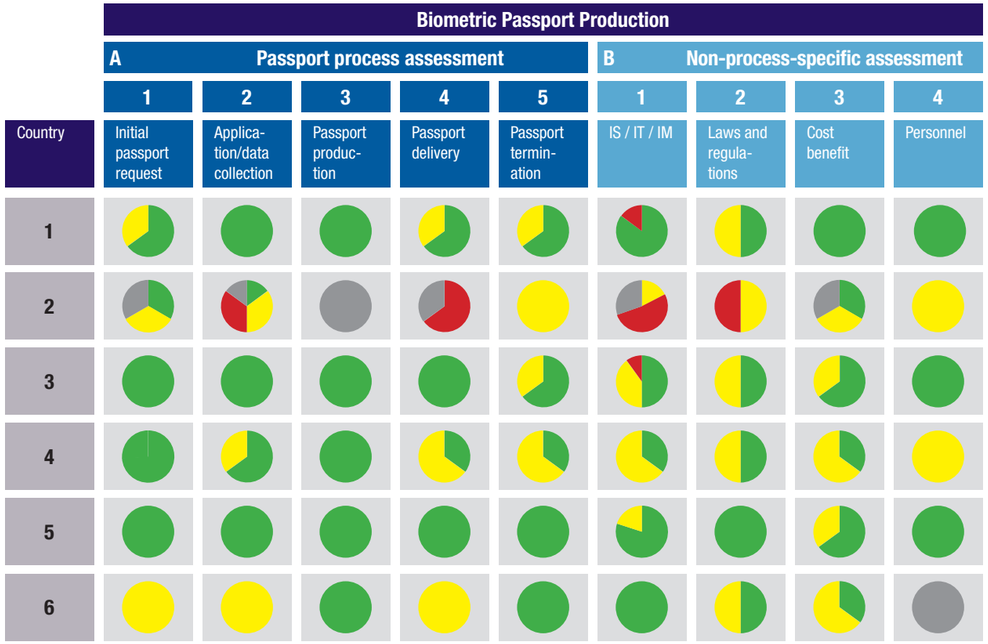


The Parallel Audit on Biometric Passport production was performed by the participating countries in four different phases and according to the following timetable:

1. Planning phase
2. Execution phase
3. Reporting deadline
4. Period of data considered for the audit



# Overview of results






# Interpretation of results

In an attempt to summarise and comment on the overall results of the Parallel Audit on Biometric Passports, the following main aspects have been identified as being important and deserving of consideration. They cover some common weaknesses and strengths by audit area:

## Passport process assessment

- Initial passport process: The initial passport request process functions reasonably well in nearly all countries, with only very few exceptions concerning authorisation, quality and exception handling.
- Application and data collection: The application and data collection procedures show some major weaknesses in one specific country. The risks involved are the following: identification of the wrong person, the misuse of data and poor validation of ID documents due to a lack of equipment. Additionally, weak access controls for the national passport database, computers and software used for passport application processing have been found. A couple of countries identified medium risks as to the quality of gathered data and data which do not meet the requirements.
- Passport production: The process of producing passports is assessed in all countries as having low or no risks. Various controls are in place throughout the passport production process.
- Passport delivery: The delivery of passports seems to be at a higher risk level than passport production. One major weakness is the postal service or, more precisely, the lack of controls to immediately detect loss or theft of passports during the delivery process. One country reported that no unified approach with respect to the activation and registration of dispatched documents is in place in the information system.
- Passport termination: The passport termination processes are affected by several medium-risk aspects in various countries. In certain situations, it is possible that invalid passports are not mandatorily revoked. Weaknesses in the destruction process and the risk that passports initially reported lost can be revalidated were also part of the findings. In one country, ID documents lost abroad were not always reported to the competent authorities of that country, which entails the risk that a person's identity document could be used illegally. One specific audit finding relates to the lack of clear terms concerning the storage and destruction of applications and electronic information of passports in the database.

## Non-process-specific assessment

- IS/IT system and management: The main weaknesses in this area consist of missing or incomplete information-security concepts, inappropriate or missing backup facilities, deficiencies in monitoring policies, standards and procedures, as well as limitations in the availability of IT systems. Significant risks are identified with regard to information security and the lack of systematic risk assessments. Weak access management and access controls were reported together with inappropriate access rights. Regarding policies and standards, there is a lack of definition of what controls should be applied to protect the data during production and by whom. Furthermore, audit deficiencies were revealed in respect

to the processes of security incident monitoring.

- Laws and regulations: In some countries, non-compliance with national legislation regarding personal data has been identified as well as non-compliance with requirements of IS/IT management legislation. It was found that the requirements of some regulatory decrees are not strictly established and are applied according to an oral rather than a written agreement.
- Cost-benefit: In some cases, no assessment of the cost effectiveness of the issuance of biometric identity documents (operations, security, IS/IT management) was carried out at state level. Furthermore, often there are no data available on the costs of the institutions involved in the process of issuance. Regarding transparency, the findings show that calculations of the fees relating to state documents are not clear or traceable.
- Internal and external personnel involved: In nearly all the participating countries, outsourcing providers are involved. Cases have been identified where no non-disclosure agreements with the respective bodies had been signed. Additionally, the issuing bodies do not perform in-depth inspections regarding the staff employed by service providers.



# Methodology: Lessons learned

As part of the debriefing exercise, the SFAO performed a short survey amongst the participating countries. This allowed some important lessons to be drawn for future parallel audits:

- Valuable experience of sharing and learning: Parallel audits in general facilitate sharing and learning (new) practices. All of the countries thought that their participation in this parallel audit was worthwhile and interesting. Most of them had never been involved in such an audit before and found many benefits in sharing audit procedures as well as the final results.
- Right approach: The chosen approach allowed the audit to be performed within the defined scope and provided for relevant findings in the area of biometric passports.
- Preparatory activities by leading country: The Common Audit Programme and the Audit Instructions were established by the SFAO. The participating countries appreciated this preparatory work, as it helped to save time as well as resources and provided a common focus.
- Involvement of participating countries is important: The definition of risk areas in the Common Audit Programme was perceived as a significant benefit. Additionally, the comparison of results with those of other countries was appreciated. Sharing ideas and fixing audit-specific details during the preparation phase was also recognised as being helpful. Detailed minutes of the working meetings (conference calls) were also considered useful.
- Different national realities to be covered: A parallel audit allows a focus on the main audit topics relevant to different countries and the application of a common methodology to different national realities. Some of the countries adapted the Common Audit Programme to cover their local situation and to comply with national procedures, requirement and standards. However, this tailoring was perceived as challenging. In addition, it was felt that there was some lack of practical examples or best practices for evaluating processes.
- Parallel audit in itself is a challenge: The participating countries recognised that preparing, planning and performing a parallel audit is more challenging than executing an individual local audit.
- KPIs would be useful: With regard to potential improvements, the participating countries suggested developing clear key performance indicators (KPIs). This would contribute to better performance measurements and comparisons.
- Common assessment criteria: In addition to the COBIT criteria, further common assessment criteria would be a valuable input in a next parallel audit.
- Timeliness of communication: The participating countries would have preferred to share findings, experiences and primary results more systematically during the execution phase and not only towards the end of the audit.
- Use of current COBIT framework: Finally, the participating countries also suggested the use of COBIT 5 for future parallel audits instead of the previous 4.1 version.
- In summary, the participating countries perceived this parallel audit as a very rewarding exercise. Implementing these lessons learned in future parallel audits will improve the overall audit approach and provide better support to audit teams.