INCERT GIE

Information security approach for delivering business services

1. INCERT GIE overview

Current roles

1. **Managing IT infrastructures** on behalf of the State of Luxembourg.
2. **Personalizing smart cards** as well as **PIN and PUK codes letters**.
3. **Assisting** Luxembourgish public administrations with regard to **travel and secure documents** (ePassport, eResidence Permit and eID card).
4. **Representing Luxembourg** at international standardisation committees within **specific information security domains** (e.g. PKI, aviation security and cyber security).

A little bit of history…

- **Created "on the paper" in August 2012** by the **State of Luxembourg** and the **Luxembourg Chamber of Commerce.**
- **Started "operationally" in January 2013 with 2 employees.**

2. INCERT GIE business services

INCERT GIE is **transversally serving 3 Luxembourgish ministries**.

Management of **public critical IT infrastructures** (role 1)

LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie

LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère des Affaires étrangères et européennes

LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Intérieur et à la Grande Région

ePassport

eResidence Permit

eID card

Country Signing Certification Authority (CSCA)

- Digital signing the personal data contained in the contactless chip of each Luxembourgish ePassport, eResidence Permit and eID card to guarantee the authenticity of these data.

Country Verifier Certification Authority (CVCA) // Document Verifier Certification Authority (DVCA)

- Protecting and regulating the access to the sensitive data (e.g. fingerprints, social security number) of each issued eDocument.

National Public Key Directory

Single Point of Contact

EUROPEAN COMMISSION

NPKD

- Handling a **trusted list of certificates** published by member countries of the ***International Civil Aviation Organisation*** and making this list available to the Police and border control to enable them to verify the authenticity of ePassports issued by foreign countries.

SPOC

- Managing the access requests from foreign countries to the fingerprints of the Luxembourgish ePassports and eResidence Permits.

A unique centre of expertise in **PKI technology supporting travel and secure documents**.

2. INCERT GIE business services

INCERT GIE also acts as a **PKI operator for private organisations**.

Management of **public critical IT infrastructures** (role 1)

LUXTRUST

regify
your mail matters

National Public Key Infrastructure

NPKI

- Providing a **set of PKI modules** to LuxTrust (Luxembourgish Certification Authority) to enable this organisation establishing and running **qualified and SSL Certification Authorities, and Time Stamping Authorities**.

Business information	Amounts
Number of OCSP tokens generated in Year 2014:	~96 000 000
Number of downloaded CRLs in Year 2014:	~219 000 000
Number of connexions per second for OCSP/CRLs:	Approx. 180
Number of countries from which CRLs are downloaded on a monthly basis:	Over 170

Clearing Centre

Clearing Centre

- **Securely storing encryption/decryption keys** used by Regify clients to exchange sensitive information through "**Regimail**" products.

Business information	Amount
Number of "Regimail" transactions generated in Year 2014:	~175 000

An organisation **providing business services that are client oriented**.

3. INCERT GIE information security strategy

Back in January 2013, first objectives of INCERT GIE were to:

- **Take over and handle existing IT infrastructures** (e.g. NPKI, ePassports PKI) now under its responsibility;
- **Plan the deployment of new ones** (e.g. NPKD, SPOC); and
- **Establish a comprehensive and pragmatic information security and operational strategy** for being able to manage both previous objectives.

Therefore, a management decision was made to implement an **Information Security Management System** in accordance to the **ISO/IEC 27001 standard**.

One year later (in January 2014), INCERT GIE became the first "parapublic" organisation being certified in Luxembourg, and for **all its business and internal activities**.


BUREAU VERITAS
Certification

INCERT GIE
IVY Building, 13-15 Parc d'activités, L-8308, Capellen, Luxembourg

Bureau Veritas Certification Holding SAS - UK Branch certify that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standards detailed below

Standard

ISO/IEC 27001:2013

Scope of certification

INCERT GIE ISMS scope covers the management and supervision of critical IT infrastructures from the State of Luxembourg, including the National PKI, governmental PKIs and CAs linked to secure documents, and the Clearing Centre, as well as the personalization of smart cards and of PIN and PUK codes letters, and consultancy activities for governmental agencies.

Statement of Applicability, version 1.1 dated 4 December 2014

Certification cycle start date: 8 January 2014

Subject to the continued satisfactory operation of the organisation's Management System, this certificate expires on: 7 January 2017

Original certification date: 8 January 2014

Certificate No. IND14.1002U

Version 2, Revision date: 16 February 2015

Signature

Signed on behalf of BVCH SAS UK Branch

UKAS

008

Certification body address: 66 Prescot Street, London E1 8HG, United Kingdom

Local office: Bureau Veritas Certification France

46, avenue de Général de Gaulle – Immeuble le Guilloutet – 92040 Paris La Défense

Further clarifications regarding the scope of this certificate and the applicability of the management system requirements may be obtained by consulting the certification body.

To check this certificate validity please call: +33 (0)1 41 97 44 66

Page 1 of 2

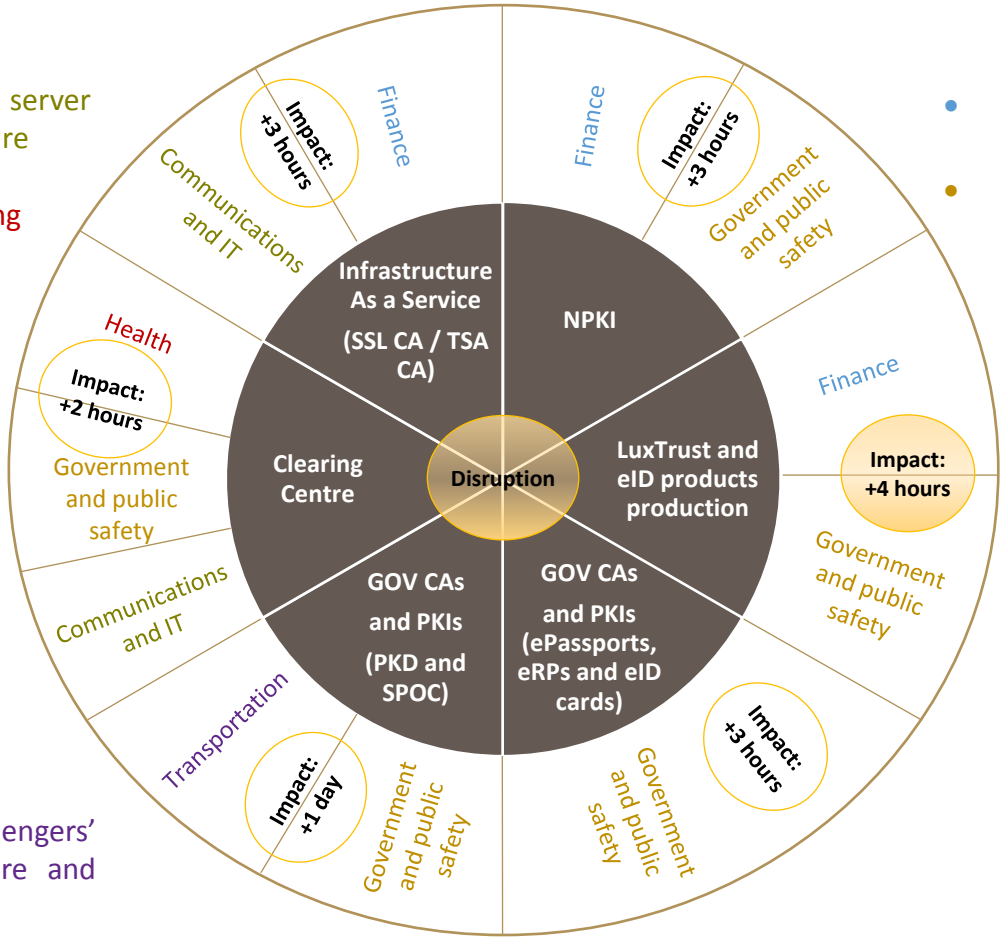
Being ISO/IEC 27001 certified **does not mean having reduced the security and operational risks to zero, but having defined, implemented and maintaining**:

- A **risk-based approach** to manage its business.
- A set of **policies and procedures**, as well as of **measures** to protect its business.

3. INCERT GIE information security strategy

A **risk-based approach** of the public critical IT infrastructures considering **the sectorial impacts** (*in terms of hours*).

- Communications and IT: server authentication and secure messaging.
- Health: secure messaging



- Finance: payment and tax processing systems.
- Government and public safety: user authentication systems, and issuance and verification of travel documents.

- Transportation: passengers' transit (usage of secure and travel documents).

INCERT GIE business services interdependency wheel

3. INCERT GIE information security strategy

A set of **policies and procedures** reflecting INCERT GIE commitment in **establishing a pragmatic cyber security approach, which covers the following layers:**

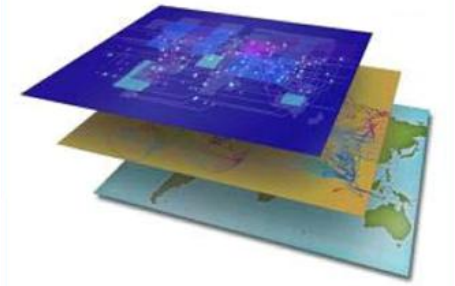
Physical Layer

Geographic Components

Physical Network Components

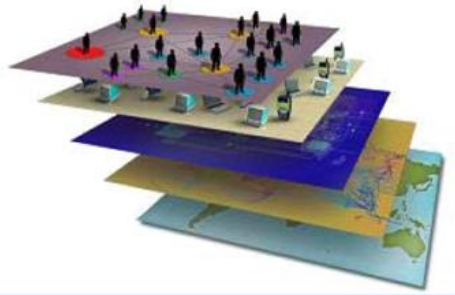
Logical Layer

Logical Network Components

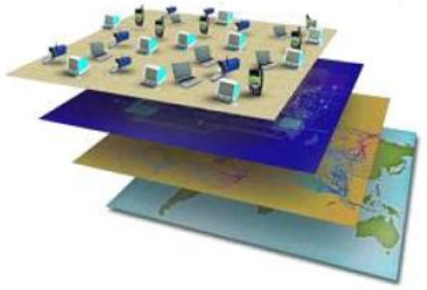


Social Layer

Cyber Persona Components



Persona Components



Source: *please contact us*.

3. INCERT GIE information security strategy

A set of **policies and procedures** adapted to INCERT GIE approach in **supplying its business services**.

Example

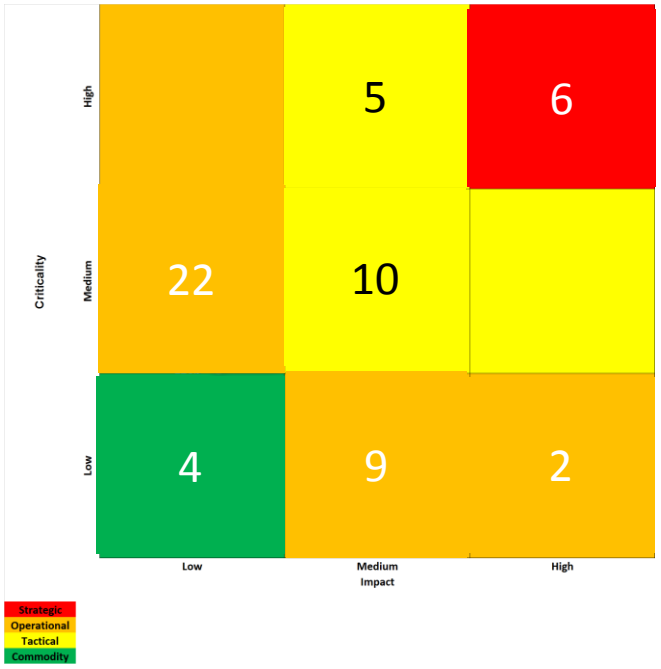
INCERT GIE current situation

About **100 suppliers**

4 acquirers

Representing more than **100+ contractual agreements**

The **supply of services** is a key element of INCERT business model



INCERT response

Supplier and acquirer relationship management

- Process defined in a policy and managed through a dedicated summary file (excel)
- Applicable to all suppliers of services/products and all acquirers
- To be followed by all INCERT employees and external ones working for INCERT

3. INCERT GIE information security strategy

A set of **technical security measures** adapted to **INCERT GIE cyber security approach**.

Proactive measures

Darknet monitoring

Hypervisor

Defence measures

Intrusion detection system

Intrusion prevention system

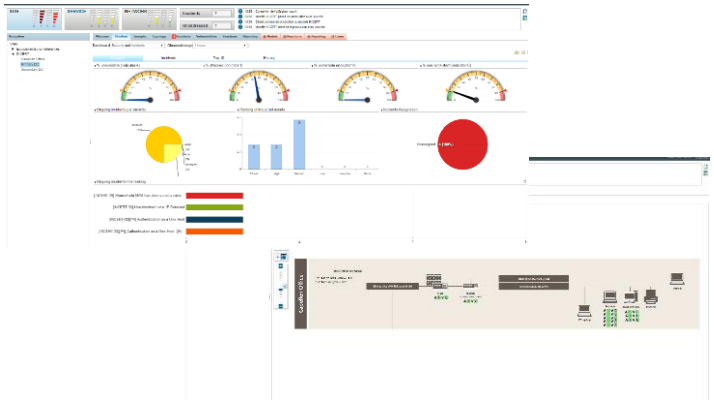
Vulnerability scanning

Secure devices

Infrastructures measures

Redundancy of key IT components and in energy / telecommunication supply

Sample of technical security measures



Precedence for the acquisition of products and services "made in Europe".

Secure phone case for reducing EM radiation (security AND safety)

Secure drive and USB key

4. Questions / Answers

Any questions ?