ALJB-ALCO Conference

CSSF's AML/CFT Risk-Based Approach (RBA) for the Banking Sector

13 November 2018

AGENDA

1. Context, Legal Basis and International Guidance
2. Risk
3. Understanding Risk
4. Mitigating Risk

RBA in a Nutshell

Focus

CSSF's RBA for ML/TF in the banking sector builds upon other RBA and is itself embedded into broader AML/CFT frameworks. Our exclusive focus today is with CSSF's RBA for ML/FT in the banking sector.

CSSF has devised analogous arrangements for entities other than banks that fall under its remit.

1

Context, Legal Basis and International Guidance

Legal Basis

Article 8-1(4) of the law of 12 November 2004 on the fight against money laundering and terrorist financing

"The supervisory authorities and self-regulatory bodies shall apply a **risk-based approach to supervision**. When applying this approach, the supervisory authorities and self-regulatory bodies shall:

(a) ensure that they have a clear understanding of the risks of money laundering and terrorist financing present in Luxembourg;

(b) have on-site and off-site access to all relevant information on the specific domestic and international risks associated with customers, products and services of the professionals; and

(c) base the frequency and intensity of on-site and off-site supervision on the risk profile of the professionals, and on the risks of money laundering and terrorist financing in Luxembourg."

Legal Basis

Article 8-1(4) of the law of 12 November 2004 derives from DIRECTIVE (EU) 2015/849 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC transposes Directive into LU law the fight against money laundering and terrorist financing

According to the recitals:

(22) The **risk** of money laundering and terrorist financing **is not the same** in every case. Accordingly, a holistic, risk-based approach should be used. The risk-based approach is not an unduly permissive option for Member States and obliged entities. It involves the **use of evidence-based decision-making** in order to target the risks of money laundering and terrorist financing facing the Union and those operating within it more effectively.

(23) Underpinning the risk-based approach is the need for Member States and the Union to identify, understand and mitigate the risks of money laundering and terrorist financing that they face.

International Guidance

1. **FATF Guidance for a Risk-Based Approach**. The Banking Sector (October 2014)

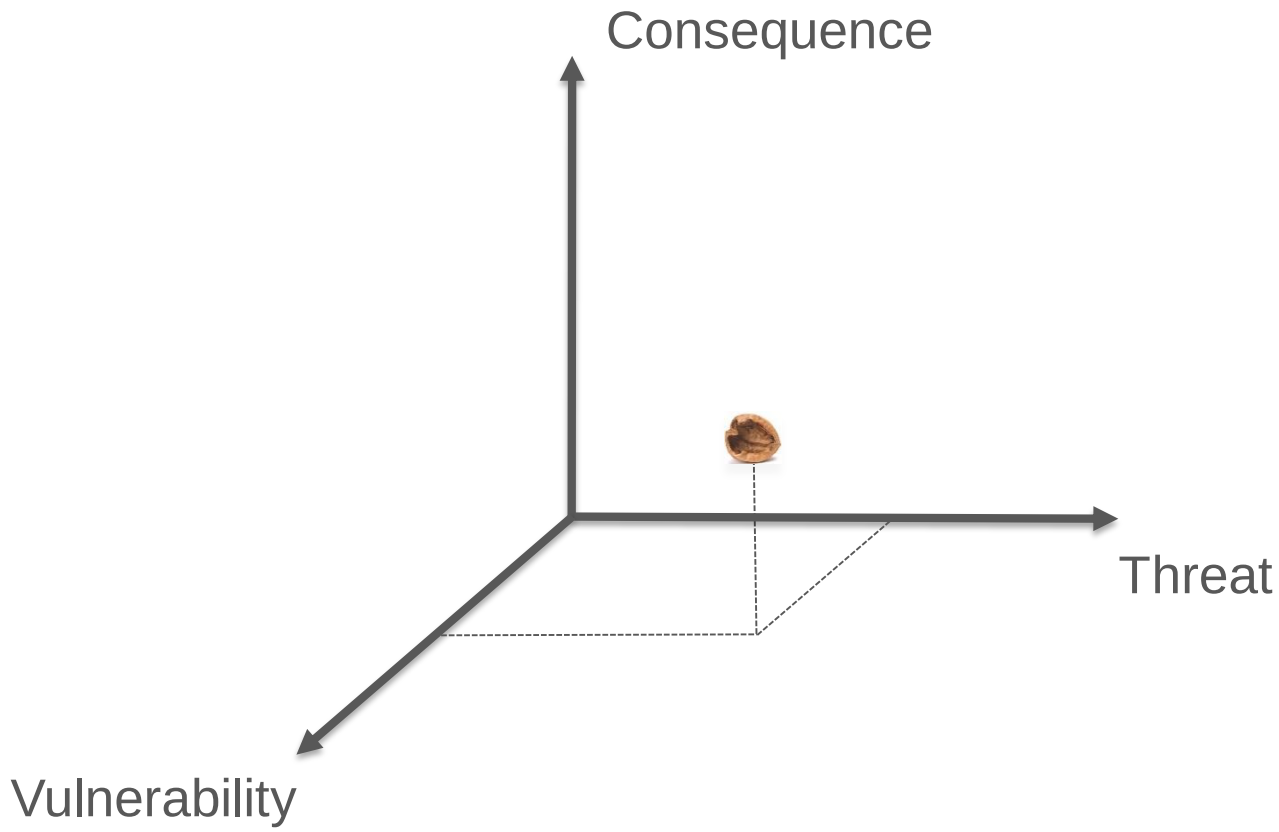
   "RBA means that countries, competent authorities and financial institutions, are expected to identify, assess and understand the ML/TF risks to which they are exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively." (§9)

2. The **ESAs Risk-Based Supervision Guidelines** (April 2017)

   "set out the characteristics of a risk-based approach to anti-money laundering and countering the financing of terrorism (AML/CFT) supervision and the steps competent authorities should take when conducting supervision on a risk-sensitive basis." (§1)

2 Risk

The Risk Space



FATF Guidance « National Money Laundering and Terrorist Financing Risk Assessment », February 2013

Risk Factors

1. Threat

Person or group of people, object or activity with the potential to cause harm to, for example, the state, society, the economy, etc. In the ML/TF context this includes criminals, terrorist groups and their facilitators, their funds, as well as past, present and future ML or TF activities [§10]

Sources for risk identification and assessment: domestic and international statistics, intelligence and analysis (in particular risk assessments and typologies); exchange with other authorities; CSSF supervision

Risk Factors

2. Vulnerability

Things that can be exploited by the threat or that may support or facilitate its activities [§10]

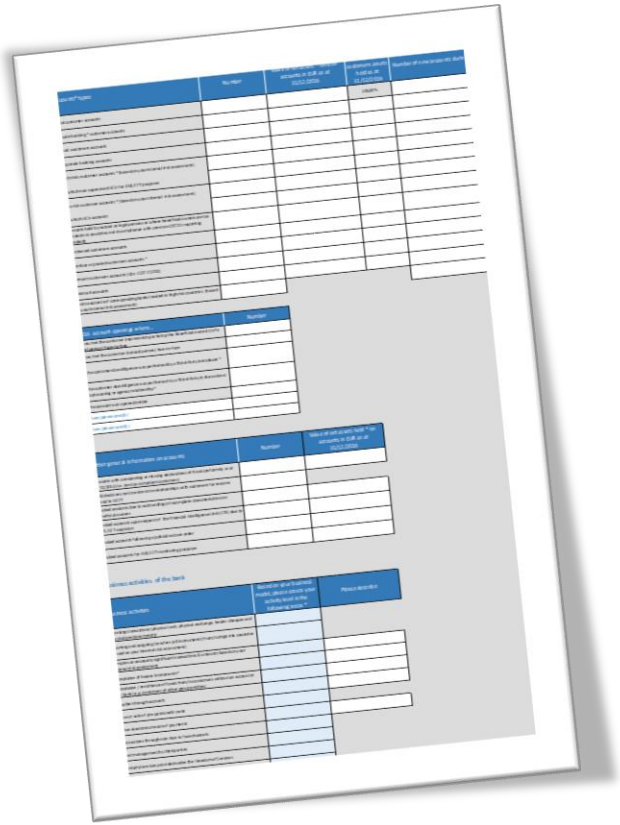
Banks

- ⇨ Financial product or type of service
- ⇨ Weaknesses in banks' AML/CFT frameworks

Source for risk assessment: CSSF supervision

- ⇨ Annual AML/CFT questionnaires

Annual AML/CFT Bank Questionnaire



Risks divided in **5 sub-categories**:

1. Geographical risk
2. Business activities
3. Accounts of clients
4. 2017 transaction activity
5. AML/CFT fines and litigations, suits

Mitigation measures divided in **6 sub-categories:**

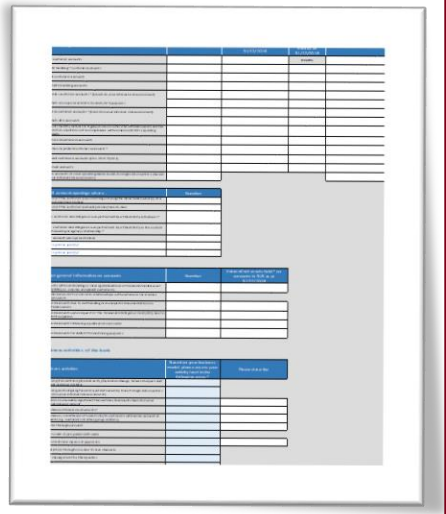
1. ML/TF risk assessment, risk management and mitigation
2. AML/CFT policies and procedures
3. AML/CFT internal controls and governance
4. IT monitoring tools
5. Staffing
6. AML/CFT Training

Annual AML/CFT Questionnaires

2018

1 General banking activities

2 Depositary / Custody activities for UCIs



2018

4 Trust and Company Service Provider activities

3 Transfer Agent activities for UCIs

Risk Factors

3. Consequence

Impact or harm that ML or TF may cause and includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society more generally [§10]

…

Risk Factors

3. Consequence

Given the challenges in determining or estimating the consequences of ML and TF it is accepted that incorporating consequence into risk assessments may not involve particularly sophisticated approaches, and that countries may instead opt to focus primarily on achieving a comprehensive understanding of their threats and vulnerabilities. [§10]

➔ (May be) used as a determinant to prioritize mitigating measures.

3 Understanding Risk

Ranking Risk

Higher risk seen on aggregate as related to

1. Money laundering (rather than proliferation or terrorism)
2. Proceeds of foreign crimes (rather than domestic ones), non-resident clients, in particular those from higher risk countries
3. Corruption and bribery, fraud and forgery, tax crimes, drug trafficking, organized criminality and racketing, counterfeiting and piracy of products, sexual exploitation and smuggling (as compared to other designated predicate offences) and clients with higher risk exposure to such predicate offences

Ranking Risk

Related banking sector vulnerabilities are higher in

1. Private Banks/Private Banking (as compared to other banking activities)
2. Products and services with a high level of privacy
3. Banks with a higher risk appetite/weaker internal control culture

! Caveat: Banks' RBA may legitimately imply a focus on risks not mentioned on slides 17 and 18 !

Scoring Risk

CSSF's ML/TF Risk Matrix and Grading

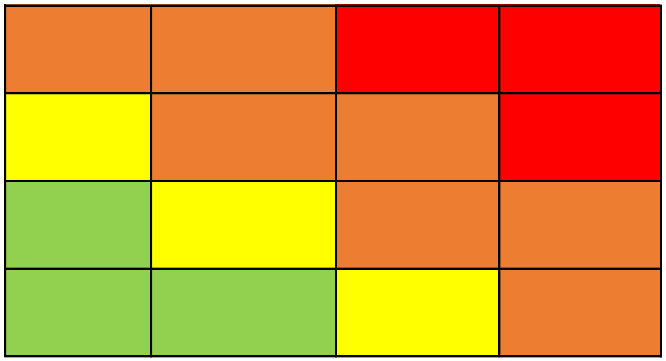
Risk Exposure

High 4. High

3. Medium high

2. Medium low

Low 1. Low

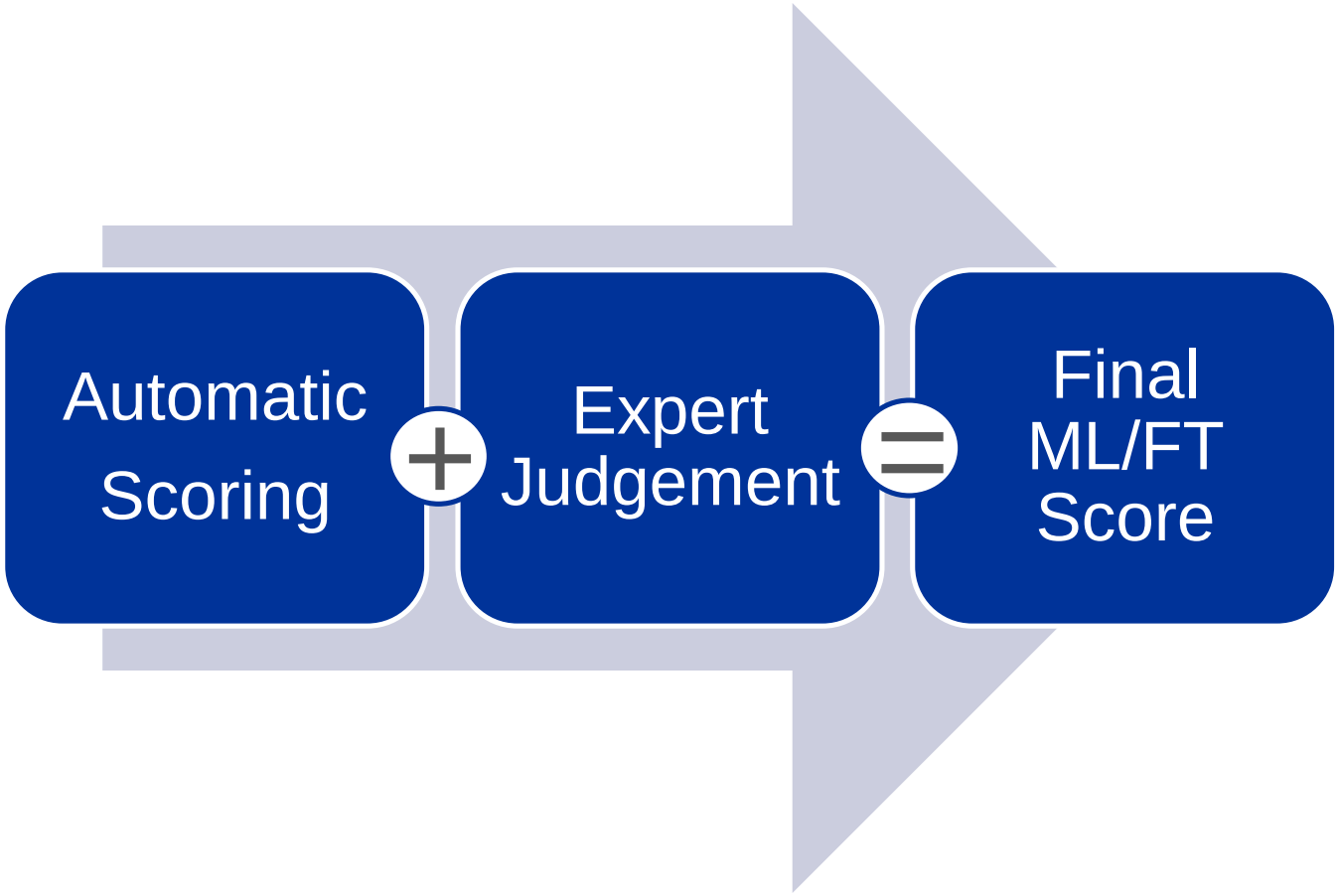


1. High 2. Substantial 3. Moderate 4. Low

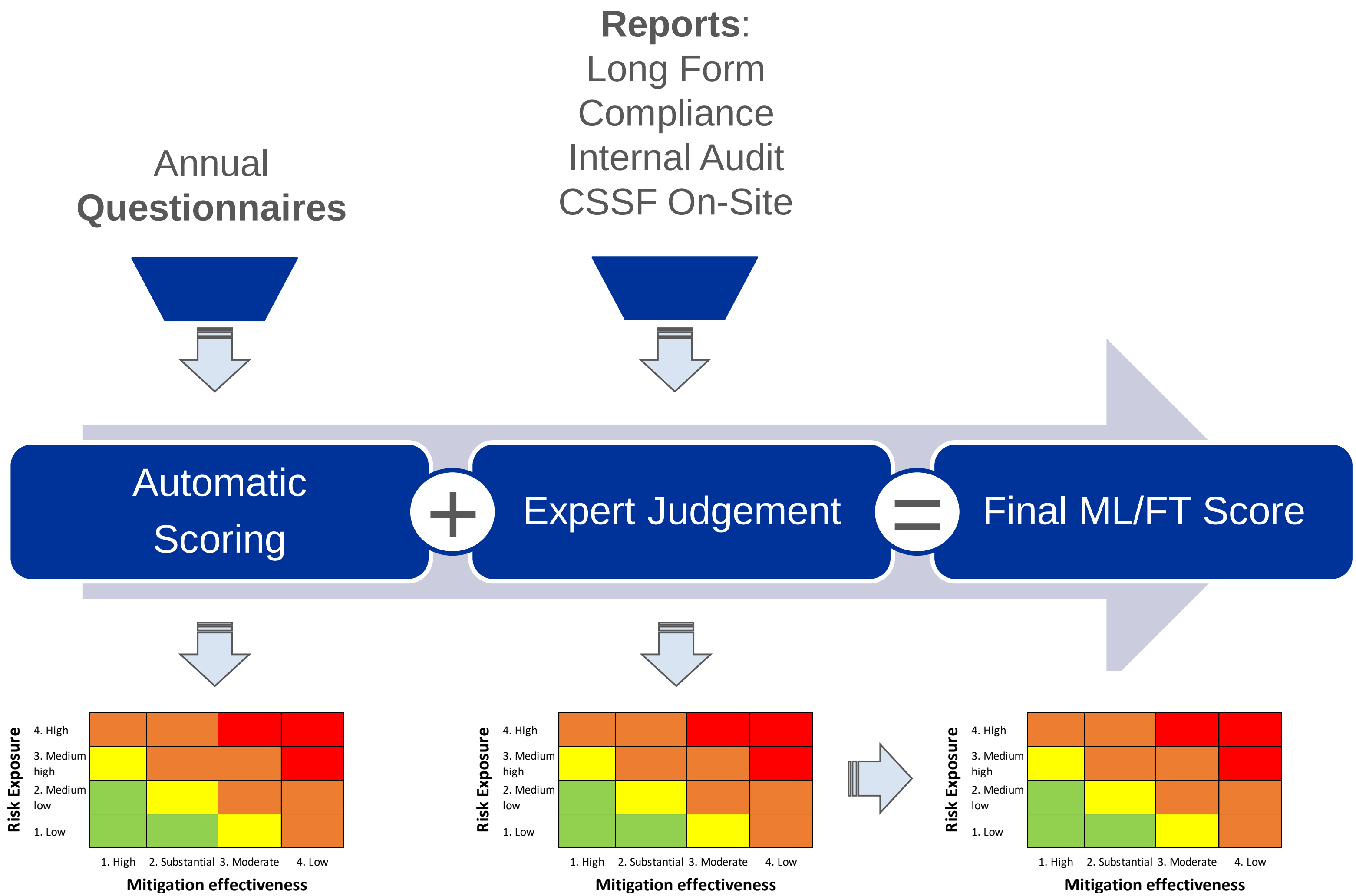
High **Low**

Mitigation effectiveness

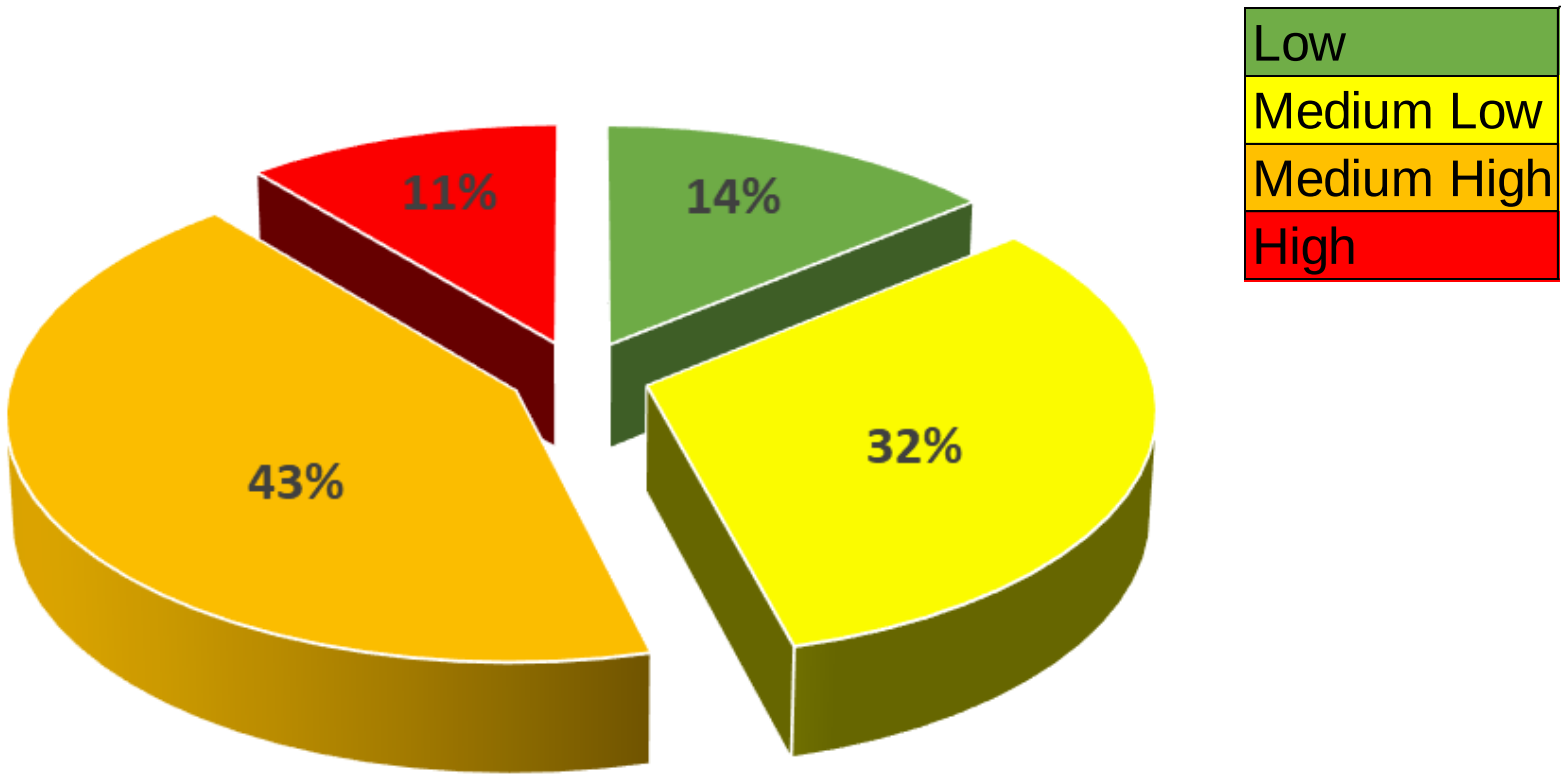
Scoring Risk



Scoring Risk



Current Risk Scores



4 Mitigating Risk

Supervisory Examination Programme

1. Multi-year, risk-sensitive supervisory plan
2. Frequency & intensity of supervision increase with risk score

3. Off-site & onsite (reporting, interviews, inspections, tailored supervisory measures & follow-up)
4. Focus adjusted to institution or sector-related developments
5. Guidance: CSSF 12-02, CSSF Circular 17/650, Q&A's on CSSF website, FATF guidance

On-site Inspections (OSI's)

- N.B. Institutions covered by OSI's : Banks, Investment firms, PSF's, ManCo's, Investment Funds
- OSI Definition : OSI's are in-depth investigations; duration of several weeks
- Preparation phase – Field work – Reporting phase – Communication phase
- OSI Department responsible for Banks, Investment firms, PSF's (20 FTE)
- CSP OPC Department responsible for ManCo's (4 FTE)
- Final validation meeting

On-site Inspections (OSI's)

- Full scope OSI
- Follow-up OSI
- Ad hoc OSI
- 2019: thematic modular or targeted inspections <-> peer reviews and communication with private sector on results and CSSF's expectations
- 2019: CSSF OSI RBA <-> varying intensity level, varying frequency
- 2019: enhanced focus on terrorism financing
- 2019: enhanced focus on RBA (governance, definition of risk appetite, mitigation measures)
- Commonly used OSI techniques : analysis of procedures, management interviews, walk-through, tests on a sample basis
- Interventions means : observation letter, injunction letter, enforcement

Enforcement

- Legal basis has changed : Article 63 (2) Law on FS 1993 – Article 8-4 Law AML 2004 – higher sanctioning amounts are possible
- Injunction article 59 law FS 1993 still applicable
- Administrative sanctions Art 8-4 Law AML 2004 -> possible actions CSSF : warning, blame, withdrawal or suspension of license, temporary interdictions of professional activity (< 5 years), financial sanction (2x amount of advantage or max 1 Mio EUR)
- Administrative sanctions Art 8-4 Law AML 2004 for banks or financial institutions-> up to 5 mio Eur or 10% of annual turnover for legal persons ; up to 5 Mio Eur for natural persons
- Financial sanction of 250-250.000 Eur foreseen if non respect of injunction, prohibition to prudential supervision of the CSSF, communication of wrong information

Enforcement

- Factors to be taken into account :
  - Gravity and duration of legal violations
  - Degree of responsibility of legal/natural person
  - Financial situation of legal/natural person
  - Advantage taken out of violation by legal/natural person (if possible to determine)
  - Harm suffered by third parties (if possible to determine)
  - Degree of cooperation of legal/natural person
  - Recurrence of violation done by legal/natural person
  - Systemic consequences of the violation
- Proportional <-> Dissuasive sanctions
- Mandatory nominative publication of the sanction
- Possible recourse against decision within one month from notification

Enforcement

CSSF enforcement approach after an OSI

- Substantiation of the findings during OSI
- Fact validation meeting after on-site phase and before issuing observation letter
- Internal scoring tool of the weaknesses detected-> observation letter, injunction, enforcement
- PANC1 letter
- Right to be heard
- Presentation of action plan
- Analysis of institution’s response to PANC1 letter
- Final decision of CSSF
- Publication
- Possible recourse

Thank you for your attention!