



SHIFT2RAIL ANTI FRAUD  
STRATEGY 2017-2020  
(EXTENDED UNTIL 31  
DECEMBER 2021)

---

## Table of Contents

<b>1</b>	<b>Background</b> .....	<b>3</b>
<b>1.1</b>	<b>General context</b> .....	<b>3</b>
<b>1.2</b>	<b>Shift2Rail Joint Undertaking context</b> .....	<b>3</b>
<b>1.3</b>	<b>Definitions</b> .....	<b>5</b>
<b>2</b>	<b>Fraud risk assessment</b> .....	<b>6</b>
<b>3</b>	<b>Means and resources</b> .....	<b>7</b>
<b>3.1</b>	<b>Human resources</b> .....	<b>7</b>
<b>3.2</b>	<b>IT tools</b> .....	<b>7</b>
<b>3.3</b>	<b>Specific procedures, networks and trainings</b> .....	<b>7</b>
<b>3.4</b>	<b>Objective 1: MAINTAIN A CULTURE OF INTEGRITY AND BUILD CAPACITIES THROUGH TRAINING AND GUIDANCE</b> .....	<b>9</b>
<b>3.5</b>	<b>Objective 2: ENSURE A HIGH LEVEL OF REACTIVITY</b> .....	<b>9</b>
<b>3.6</b>	<b>Objective 3: PREVENT DATA LEAKAGE</b> .....	<b>10</b>
<b>4</b>	<b>INDICATORS</b> .....	<b>10</b>
<b>5</b>	<b>ACTION PLAN</b> .....	<b>11</b>

# 1 Background

## 1.1 General context

The EU budget is taxpayer's money that must be used only for implementing the policies, which the EU legislature has approved. Fraud involving EU funds has a particularly negative impact on the reputation of the Commission institutions and the implementation of the EU policies.

On 24 June 2011, the Commission has adopted its new Anti-fraud Strategy (CAFS)<sup>1</sup>, its overall objective being to improve prevention, detection and the conditions for investigations of fraud, to achieve adequate reparation and deterrence, especially by developing close cooperation and synergies and promoting the standards set out in the CAFS within the EU agencies and bodies, including joint undertakings.

The Commission has developed a Common approach on EU decentralised agencies that provides for a set of anti-fraud measures to be put in place in the Agencies.

## 1.2 Shift2Rail Joint Undertaking context

### The S2R JU core activities

The Shift2Rail Joint Undertaking (hereinafter referred to as the S2R JU) was established in 2014 as a new public-private partnership in the rail sector<sup>2</sup>.

S2R JU is the first European rail joint technology initiative (JTI) to seek focused research and innovation (R&I) and market-driven solutions by accelerating the integration of new and advanced technologies into innovative rail product solutions. Shift2Rail will promote the competitiveness of the European Rail Industry and will meet the changing EU transport needs. Through the R&I carried out within this Horizon 2020 initiative, the aim is to create the necessary technology to establish a Single European Railway Area (SERA).

The Shift2Rail programme is structured in five asset-specific Innovation Programmes (IPs), covering all the different technical and functional (process) subsystems of the rail system:

- IP1: cost-efficient and reliable trains, including high-capacity trains and high-speed trains;
- IP2: advanced traffic management & control systems;
- IP3: cost-efficient, sustainable and reliable high-capacity infrastructure;
- IP4: IT solutions for attractive railway services;

---

<sup>1</sup> Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee, the Committee of the Regions and the Court of Auditors on the Commission anti-fraud strategy, COM(2011)376; Communication to the Commission : Commission internal action plan for the implementations of the Commission anti-fraud strategy, SEC(2011)787.

<sup>2</sup> Council Regulation (EU) No 642/2014 of 16 June 2014 establishing the Shift2Rail Joint Undertaking

IP5: technologies for sustainable & attractive European freight.

In addition, horizontal activities are performed through the Cross Cutting Activities.

The budget is mostly implemented through grant agreements. The main partners of the agency are the S2R JU Members other than the Union.

### The S2R JU Budget

The S2R JU Budget is governed by Articles 3 and 4 of Council Regulation (EU) No 264/2014 of June 16<sup>th</sup>, 2014<sup>3</sup>, establishing the Shift2Rail Joint Undertaking and disbursed as follows:

- 5-8% through procurements on operational and administrative expenditures; of which budget associated to risk of fraud is being mitigated by the S2R JU anti-fraud strategy
- 92-95% through grant agreements; of which budget associated to risks of fraud is being mitigated by the H2020 anti-fraud strategy

### Anti-Fraud measures

Anti-fraud measures are an essential element of the legal and financial framework of the Shift2Rail Joint Undertaking. The JU therefore thoroughly implements following measures ensuring its sound financial management and inherently addressing fraud risks:

- For H2020 projects, the S2R JU uses the H2020 tools provided for Grant Management and works in full compliance with the Financial Regulation, the Rules for Participation that establish the obligations under which the S2R JU undertakes its work and the H2020 anti-fraud strategy.
- The principle of sound financial Management which involves reducing the risk of fraud and irregularities by building relevant preventive and protective measures in the Internal Control Systems (Articles 11 and 12 of the S2R JU Financial Rules<sup>4</sup>).
- According to Article 16 (paragraph 1, subparagraph 2) of the S2R JU Financial Rules the JU shall participate in fraud prevention activities of the European Anti-Fraud Office (OLAF).

---

<sup>3</sup> <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0642>

<sup>4</sup> [https://shift2rail.org/wp-content/uploads/2016/01/S2R-JU-GB\\_Decision-N-21-2015-revised-financial-rules.pdf](https://shift2rail.org/wp-content/uploads/2016/01/S2R-JU-GB_Decision-N-21-2015-revised-financial-rules.pdf)

## 1.3 Definitions

### *Definition of Fraud:*

According to the definition used by OLAF, Fraud<sup>5</sup> covers a range of irregularities and illegal acts characterized by intentional deception or misrepresentation, damaging the interests of the EU. Fraud differs from 'irregularity'<sup>6</sup>, which is an act which does not comply with EU rules and which has a potentially negative impact on EU financial interests, but which may be the result of genuine errors committed by beneficiaries claiming funds or by the authorities responsible for making payments. The concept of fraud encompasses both, internal and external misbehaviour. It covers in particular, but not only, any infringement of the financial interests of the EU as defined by the Convention on the protection of the European Communities' financial interest. It also covers misbehaviour that may not have a direct impact on the EU's financial interests, such as some cases of forgery (in CVs for example), money laundering, concealment or destruction of material facts, or breaches of IT systems. Conflicts of interests that have intentionally not been declared, favouritism and collusion also belong to the category of fraud.

### *Definition of Anti-Fraud Strategy:*

The Anti-Fraud Strategy is a framework set up primarily to prevent, but also to address the issue of fraud at S2R JU level providing the objectives of the Executive Director and the Governing Board in the fight against fraud for the next two to three years. The purpose of the Anti-Fraud Strategy is to provide management with a tool to ensure progress and transparency as regards the protection of the EU financial interests and all financial matters regardless of source, compliance with EU ethical values and therefore the protection of the EU reputation.

---

<sup>5</sup> In respect of expenditure, as any intentional act or omission relating to:

- the use or presentation of false, incorrect or incomplete statements or documents, which has as its effect the misappropriation or wrongful retention of funds from the general budget of the European Communities or budgets managed by, or on behalf of, the European Communities;

- non-disclosure of information in violation of a specific obligation, with the same effect;

- the misapplication of such funds for purposes other than those for which they were originally granted

**In respect of revenue**, as any intentional act or omission relating to:

- the use or presentation of false, incorrect or incomplete statements or documents, which has as its effect the illegal diminution of the resources of the general budget of the European Communities or budgets managed by, or on behalf of, the European Communities

- non-disclosure of information in violation of a specific obligation, with the same effect

- misapplication of a legally obtained benefit, with the same effect

<sup>6</sup> **Irregularity** is "any infringement of a provision of Community law resulting from an act or omission by an economic operator, which has, or would have, the effect of prejudicing the general budget of the Communities or budgets managed by them, either by reducing or losing revenue accruing from own resources collected directly on behalf of the Communities, or by an unjustified item of expenditure". *Council Regulation (EC) No 2988/95, Article 1 (2), OJ L 321, 23.12.1995, p.2*

## 2 Fraud risk assessment

Before setting up the Anti-Fraud Strategy and action plan, the S2R JU carried out, in Q2 and Q3 of 2017, a risk assessment exercise comprising the identification of fraud related risks, to ensure that fraud issues are closely and effectively monitored.

This fraud risk assessment involved 3 steps:

1. Identification of the risk of fraud as regards the general objectives set by the JU (see Article 2 of the Council Regulation establishing the S2R JU<sup>7</sup>);
2. Assessment and prioritising of related fraud risks;
3. Selection of main fraud exposed activities to be addressed and monitored

When carrying out the fraud risk assessment, , further to the basic elements following the European Commission's methodology and guidance for anti-fraud strategies, the S2R JU additionally covered non-financial fraud elements by taking into account the risks of serious damage to the image and reputation of the JU, the Commission and the European Union as a whole. Furthermore, it included abuse of law, corruption, money laundering, fraudulent behaviour in procurements, conflicts of interests, fraudulent behaviour in recruitment and any behaviour defined as illegal<sup>8</sup>.

The level of fraud risk itself was assessed and hierarchized following its impact and the probability of its occurrence. The impact was classified in five different categories and the probability of occurrence was ranged from 1 (lowest) to 5 (highest). Further to the assessment exercise itself, risks have been confronted to mitigating actions for the purpose of establishing the remaining risk level (net criticality) enabling the establishment of a main risk register.

The selected findings related to fraud are addressed in S2R JU 2017 Antifraud Action Plan (See Chapter 6 of the present document). Nevertheless, their existence has not been deemed serious enough for being reported in the draft Annual Work Plan 2018 submitted to the S2R JU Governing Board (October 2017).

### Main findings:

In general terms, taking into account the overall context and existing controls, the S2R JU has assessed that the risk of significant undetected fraud is limited. Nevertheless, the following risks have been identified in the context of the S2R JU Anti-Fraud risk assessment:

---

<sup>7</sup> Council Regulation (EU) No 642/2014 of 16 June 2014 establishing the Shift2Rail Joint Undertaking (OJ L 177, 17.6.2014, p. 9)

<sup>8</sup> It is to be noted that all aspects of fraud associated to grant management haven't been taken into consideration in this document as the H2020 anti-fraud strategy as defined by the European Commission is applicable and strictly followed by the S2R JU.

- R1: A member of S2R JU staff with influence over the evaluation of tenders and contract award decision has an undeclared interest in one of the competing economic operators
- R2: Deliberate, artificial increase of budget foreseen for ensuring contracts
- R3: Tender documents are drafted so as to favour a particular supplier
- R4: The same entities are invited to tender with the knowledge that the same service provider/ supplier is likely to be awarded the contract each time
- R5: One tenderer is actively invited, while other potential suppliers are ignored
- R6: Information relative to a procurement initiative is provided to only a preferred entity during administration of a call for tender.
- R7: Data leakage due to weak physical security systems or unauthorized computer network access or connexion
- R8: Lack of designated staff member as contact point with OLAF

### 3 Means and resources

The S2R JU has at its disposal means and resources which are engaged in tackling fraud. The main resources are:

#### 3.1 Human resources

	<b>Units/functions</b>	<b>Tasks related to anti-fraud issues</b>
1	Legal and procurement	Reviewing procurement contracts
2	Human resources	Training on ethics
3	Finance and Budget	Application of the 4 eyes principles, segregation of duties and S2R JU Financial Circuits

#### 3.2 IT tools

	<b>IT tools</b>	<b>Units involved</b>
1	ABAC (Workflow, SAP, Security...)	Administration and Finance

#### 3.3 Specific procedures, networks and trainings

	<b>Units/functions</b>	<b>Units involved</b>	<b>Task related to anti-fraud issues</b>
1	EC Head of Agencies network	Executive Director/HoRI/HoAF	Exchange of information
2	EC Head of Resources network	HoAF	Exchange of information, best practices

3	EC Auditnet for agencies	Accounting Correspondant	Exchange of information, best practice, presentations, methodology, red flags etc.
4	EC Inter JUs Accounting Network	Accounting Correspondant	Exchange of information
5	EC Admin/HR network	HR Officer	Exchange of information, best practices.
6	EC Network of Data protection Officers (DPOs)	Data Protection Officer	Exchange of information, best practices.
7	EC Network of Procurement Officers (NAPO)	Legal officer	Exchange of information, best practices.
8	EC Inter JUs Legal Network (IALN)	Legal officer	Exchange of information, best practices and drafting of official advice upon requests from other Networks.
9	OLAF training sessions	ALL	Participation in workshops, information sessions, training sessions related to fraud
10	OLAF General training sessions	ALL	Participation in workshops, information sessions, training sessions related to fraud



# STRATEGY

Taking into account the fraud risks screening, internally and externally with the partners, the S2R JU decided to concentrate its efforts to realise the following strategic objectives.

## 3.4 Objective 1: MAINTAIN A CULTURE OF INTEGRITY AND BUILD CAPACITIES THROUGH TRAINING AND GUIDANCE

Mitigation action - 2017 Anti-Fraud risk assessment main findings: R1, R2, R3, R4, R5 and R6.

Integrity and high standards of professional conduct are crucial for the independence and reputation of the S2R JU. By nature, in Joint Undertakings public and private interests are mixed and there is a higher likelihood of conflicts of interest, which in the case of the S2R JU has been successfully managed over the duration of the Programme. The S2R JU's objective for this Anti-Fraud Strategy is to continue to promote and maintain the highest level of ethical behaviour amongst staff, project leaders and S2R JU Members. This starts with an adequate tone at the top cultivating an organizational culture that does not tolerate fraud, malfeasance and other forms of corruption and will include looking at lessons learned.

To ensure that managers and staff members are aware of their responsibilities regarding preventing fraud, awareness-building is of key importance. Additionally, training is vital in maintaining the effectiveness and credibility of the Strategy. Therefore, the S2R JU will focus on awareness raising actions on both ethics and fraud prevention and detection. Each staff member should be made aware of types of ethical conduct/behaviour that he/she must observe. In parallel, the S2R JU communicates relevant guidelines and procedures on how staff should react in the case they suspect fraud is committed, provided by OLAF, available in its lobby. Moreover, links to OLAF and other relevant sites will be published on the S2R JU web page.

## 3.5 Objective 2: ENSURE A HIGH LEVEL OF REACTIVITY

Mitigation action - 2017 Anti-Fraud risk assessment main findings: all risks, especially R8.

The second objective of this Strategy is to ensure a high level of reactivity in case a fraud case is suspected. This includes fostering a close collaboration with OLAF regarding the reporting of suspected fraud cases and providing full cooperation regarding cases under investigation. Therefore a procedure will be put in place on how to manage potential OLAF cases (i.e. establish what staff should do if they suspect fraud, assist OLAF in carrying out investigations by defining roles, responsibilities and an appropriate internal workflow). In parallel, the S2R JU will determine the contact person for the relations with OLAF. The contact person will maintain a register of cases examined by OLAF and a record of official correspondence with OLAF. This procedure will be formalised and published.

### 3.6 Objective 3: PREVENT DATA LEAKAGE

Mitigation action - 2017 Anti-Fraud risk assessment main findings: R7.

Loss, misuse, modification, or unauthorized access to sensitive/confidential information can adversely affect the privacy of a staff member or third party (e.g. information on selection and recruitment processes), trade secrets of a business (e.g. commercial/financial or intellectual information about a bidder in a procurement) or even the security of the S2R JU (e.g. unauthorized access/transactions) depending on the level of sensitivity and nature of the information. To limit the risk, the objective of the S2R JU is to ensure awareness of S2R JU staff on management and access of restricted, sensitive and personal data and to ensure a strictly managed process regarding access right management (Financial tool etc.). Additionally, Regulation (EC) n° 45/2001 on the Protection of Personal data applies and the S2R JU is committed to strictly follow processes and procedures imposed by the before cited regulation.

## 4 INDICATORS

Indicators will be used to report on the Anti-Fraud Strategy. The results of fraud prevention and detection activities will be reported by the Executive Director in a chapter of the annual activity report of the S2R JU presented to the Board for approval.

The following indicators will be used by the S2R JU to report on the fraud prevention and detection activities in the Annual Activity Report.

1. Number and value of contracts subject to close monitoring or additional controls due to an assessment of a high risk of fraud
2. Number (and trend in number) of files sent to OLAF for investigation
3. Time elapsed between receipt by staff or management of first information on alleged internal fraud and transmission to OLAF.
4. Time elapsed between OLAF requests for information and date when information is provided to OLAF.
5. Time elapsed between receipt of an OLAF report and the decision on recovery or disciplinary sanctions by the S2R JU

## 5 ACTION PLAN

This action plan designed to implement the Anti-Fraud Strategy of the agency covers the period from October 2017 till September 2020. The target dates are geared to the level of priority. When implementing the actions, S2R JU will take as much as possible advantage of synergies through cooperating with other Agencies or Joint Undertakings, especially the IMI JU, the BBI JU, the FCH JU, the SESAR JU, the CleanSky JU, the ECSEL JU, by sharing best practices .

The actions will cover the stages of the anti-fraud cycle: prevention, detection, investigation and corrective measures.

Operational objective 1	Priority	Unit in charge	Deadline	Indicator
<b>Maintain a culture of Integrity and Build capacities through training and guidance for S2R JU staff</b>	Ensure an ethical and anti-fraud ‘tone at the top’: ensure management regularly conveys messages on ethics and fraud prevention to staff	S2R JU ED and Management	Constant monitoring – regular communication in weekly team meetings	Number of messages conveyed by management to staff on ethics and fraud prevention
	After a fraud case is closed, set up a debriefing with S2R JU staff on best practices concerning prevention, detection and recovery	S2R JU ED and Management	Ad hoc, when required	Number of debriefing sessions with S2R JU staff on best practices after a fraud case is closed
	Continue to raise awareness and systematic focus	S2R JU ED and	Ad hoc, when	Number of

	on ethics at governance bodies of the S2R JU	Management	required	ethics awareness raising actions targeted at the governance bodies of the S2R JU
	Implement indicators regarding Fraud into Annual Activity reporting	S2R JU ED and Management	Each year once when applicable, Q2	Indicators mentioned in the AAR
	Include links to OLAF homepage and anti-fraud documentation on S2R JU Web page under the tab “functioning of the JU”	HoAF	Q4 2017	Publication of the links on the S2R JU Website
	<b>Training</b> Provide a training session to all S2R JU staff on fraud prevention	HoAF	Q2 2017 – done – to be repeated for new staff either in 2018 or in 2019 depending on staff turnover	Number of staff members that attended the S2R JU training on ethics and fraud prevention
	Organise a S2R JU training on ethics	HoAF	Q2 2017 – done – to be repeated for new staff either in 2018 or in 2019 depending on staff turnover	Number of staff members that attended the S2R JU training on ethics and fraud prevention
	HR issues:			

	- Whistleblowing - Anti harassment (ongoing?)			
	<b>Guidance</b> Communicate practical guidance to S2R JU staff on red flags, whistleblowing, how to react and how to report fraud and ensure this guidance is easy accessible (Availability of prospects in lobby, welcome pack and shared on the S2R JU website)	HoAF and Management	Q2 2017 – done  Q4 2017 – for the publication of relevant guidance on S2R website	Presence of practical guidance for S2R JU staff on red flags, how to react when they come across a potential case, how to report fraud and
	Draw up concise guidance for S2R JU staff on possible administrative and financial penalties that can be taken in cases of misconduct, irregularities and fraud	HoAF and Management	Q2 2017 - done	Possible administrative and financial sanctions and number of staff participating in OLAF & DP Workshops
<b>Operational objective 2</b>	<b>Priority</b>	<b>Unit in charge</b>	<b>Deadline</b>	<b>Indicator</b>
<b>Ensure a high level of reactivity</b>	<b>Prevention/Detection/Investigation/Corrective measures</b> Appoint a ‘person of confidence’ competent and available to guide S2R JU staff in the area of fraud (and advertise this)	S2R JU ED and Management	Q4 2017	ED Decision on nomination of contact person with OLAF
	Ensure swift transmission of key information to	S2R JU ED and	Ad hoc, when	Time elapsed

	OLAF and full cooperation during a possible investigation and make sure that precautionary, protective and recovery measures are initiated as soon as possible	Management	required	between OLAF requests for information and date when information is provided to OLAF
<b>Operational objective 3</b>	<b>Priority</b>	<b>Unit in charge</b>	<b>Deadline</b>	<b>Indicator</b>
<b>Prevent data leakage</b>	Ensure awareness of S2R JU staff on management and access of restricted, sensitive and personal data	HoAF and Management	Q2 2017 - done	Number of awareness raising actions regarding access to data and organisation of DP Workshop as well as adoption of DP related recommended processes and procedures
	Define and implement a process of access right management (Financial Systems)	HoAF and Local Profile Manager	Constant monitoring – Access rights to ABAC financial system is conditioned by the approval of the ED or the HoAF. Annual	Number of Access rights granted and periodic report on ABAC security

			independent review of ABAC security periodic validation (with DG BUDGET) – done in May 2017	
	Ensure the effective implementation of physical security measures regarding storage of sensitive data	HoAF, DPO, IT Officer, HR Officer, all S2R JU staff	Ongoing – Q4 2017 – List of processing operations requiring secure locked cupboards for hard copies established – staff awareness to be raised and ensure effective implementation	Availability of secure locked cupboards for staff dealing with sensitive data