Agency Board Meeting
26 April 2022

Board Report Number: SEPA 15/22

Annual review of risk and corporate risk register 2021

Summary: This is the annual review of risk management and corporate risk register which cover the period from 1 January to 31 December 2021. It was approved for submission to the Board at the Audit Committee meeting on 22 March.

This paper outlines the changes to the corporate risk register and work that has been carried out to improve SEPA's approach to risk management since January 2021.

The attached Corporate Risk Register details the status of risks up to end of December 2021.

The Agency Board is responsible for ensuring that SEPA identifies, assesses and manages risks.

The Audit Committee ensures that a risk management framework is in place and scrutinises SEPA's process twice a year. It also makes recommendations to the Board on improvements needed to the risk management process. The Committee highlights to the Board specific areas of risk which require Board discussion.

The Audit Committee reviews the corporate risk register twice a year. After reviewing the register in March, the Audit Committee advised that in future, the Board might prefer to receive a summary of the risk register as part of its Annual Review of Risk, instead of the full risk register. The Board is asked to confirm whether members would prefer to see the full corporate risk register or a summary of the risks in future.

It was also agreed that the Board and Audit Committee should have a formal item at the end of each meeting to consider any possible new risks.

Risks:	This paper summarises the risk management activity in SEPA which has been put in place to identify, assess and manage corporate risks.
Resource and Staffing Implications:	None
Equalities:	We will continue to monitor this work for anything that may impact on equality. We will address them through our normal activities for embedding equality and human rights through our work.
Environmental and Carbon Impact:	None
Purpose and audience of the report:	1. The Agency Board is asked to discuss this paper. 2. The Agency Board is asked to consider whether they would prefer a summary of the risk register in future Annual Review of Risk reports instead of the full risk register. Public without Risk Register appendices
Report Author:	Katie Cairnie, Senior Business Consultant, Business Strategy Jo Green, Acting Chief Executive Officer 11 April 2022
Appendices:	Official Confidential appendices removed for publication on website

Annual Review of Risk Management 2021

1. Introduction

1.1 In this report, we provide an update on how SEPA managed risk over the past year from January to December 2021. We include a summary of the risks which we have added, amended and removed from the corporate risk register.

1.2 Under normal circumstances, the Risk Management Group provides a half yearly review of risk management to the Agency Management Team and the Audit Committee in September and a full annual review in March, which is also presented to the Board in April. COVID-19 and the cyber-attack both disrupted our reporting schedule. In 2021 the annual review was presented to the Agency Management Team, Audit Committee and Board in September. It covered 15 months from April 2020 to June 2021. To get us back onto a normal reporting schedule, this review covers a full calendar year which mean there is some overlap with the previous annual review.

1.3 We have provided a copy of the corporate risk register as Appendix 1 (removed for publication on website). The risk register is made up of a risk profile card for each risk. Since the cyber-attack, we have made some changes to risk profile cards.

2. Background

2.1 The Risk Management Group directs and oversees the management of risk in SEPA. This group met on six occasions in the last year to develop SEPA's approach to risk management, review the management of risks on the corporate risk register and assess potential new corporate risks.

2.2 It is good practice to have different levels of risk scrutiny and at least one level of risk register below the corporate register. At the September Agency Management Team and Audit Committee meetings, it was agreed that we would stop separating the next level risks by portfolio and we would develop risk registers for each of the three workstreams.

3. Annual Review

3.1 Risk Management Goals 2021-2022

We set out our approach to risk management in a risk management handbook. We produced the handbook in 2018 and we review it annually. We last reviewed in June 2021. Each year, the Risk Management Group agree a set of goals for risk management for the financial year. The goals for 2021-2022 are outlined below with an update to where we are for each one at end of December 2021.

Goal		**Status**
1	Rebuild the risk management process and supporting documentation	Complete
2	Review the risks around non-compliance with legislation	Complete
3	Identify any new corporate risks resulting from the cyber-attack or the ongoing pandemic	Complete
4	Review and refresh risk management training	In progress
5	Strengthen the link between risk and resilience	Complete

2021 Goal updates

1. We have rewritten all supporting documentation and reinstated the corporate risk process. We are working on creating workstream risk registers and building them into the current review process.

2. We have reviewed all the legislation on our legal registers and considered the impacts of both COVID-19 and the cyber-attack on our ability to meet our requirements.
3. We have reviewed all of the risks on the corporate risk register and updated them in light of the cyber-attack and the pandemic. We identified one new risk in relation to reservoirs and it was added to the corporate risk register
4. We are developing two new risk management training packages. These will be available to staff later in 2022.
5. The resilience manager now sits on the Risk Management Group. We will continue to develop in this area.

3.2 Risk Management Timeline 2021

<u>January to March</u>

- The cyber-attack on Christmas Eve meant that we were unable to access any risk documentation. Key members of staff involved in the risk process were not online.
- We created draft risk profile cards from memory and took the opportunity to improve them. We also produced a new risk scoring matrix. We developed a project plan template to help people managing recovery projects. It included a section for managing risks.
- The World Economic Forum Global Risk report 2021 was published. The focus of the report was on the global pandemic and the fallout including: digital inequality; youth disillusionment; global divides and global markets. In the perceived future risks, four of the five most likely risks and three of the five highest impact risks were environmental. This highlights the importance of our One Planet Prosperity strategy.
- In March, we presented a risk management paper to the Audit Committee in lieu of the Annual Review of Risk Management. The paper detailed the issues presented by the cyber-attack, the steps taken to address risk in the meantime and outlined the next steps required to get the risk management process back online.

<u>April to June</u>

- Key risk management staff were all back online and able to access basic systems.
- We rolled out our new risk profile cards along with guidance on how to complete them.

- Using a recovered version of the corporate risk register from September 2020, we transferred the corporate risks over to the new profile cards and rescored them using the new risk scoring matrix.
- We recovered an earlier copy of the risk management handbook. We updated it to include the new process for profiling and scoring risks in time for the UKAS audit for the 17025 standard.

July to September

- Risk owners reviewed their risks and considered the impact of the cyber-attack. Some risks were rescored as a result.
- We presented the Annual Review of Risk Management for 2020 to the Agency Management Team, Audit Committee and Board in September. It spanned 15 months from April 2020 to June 2021.

October to December

- Our Scottish Government sponsor unit asked for more information about how we are managing risks. We began providing our quarterly risk register to them. This means the Agency Management Team is now reviewing the corporate risk register quarterly instead of every six months.
- We reinstated the risk aide-memoire for the Audit Committee. This provides members with a list of the current corporate risks and their scores to refer to at the Audit Committee meetings where there is no corporate risk register on the agenda.
- We began work on two risk training packages. One for managers and other people interested in risk management and one to help people fill out risk profile cards.
- We carried out a systematic review of the legislation on our corporate legal registers to check that we understood all areas of risk. This work relates to R012.

3.3 Risk management look ahead

- The Risk Management Group will discuss and agree the Risk Management goals for 2022 in March prior to the start of the financial year. These will incorporate feedback provided by the Chair of the Audit Committee.
- We will complete our annual review and update of the Risk Management Handbook and include the goals for 2022.
- The Agency Management Team will hold a workshop to consider risks around the delivery of the 2022-2023 Annual Operating Plan.
- In January 2022, the World Economic Forum published the Global Risk report 2022. There are two main global challenges outlined in this year's report: Lack of implementation of what was agreed at COP26 and achieving net zero; and Inequality and the social crises. In this report, risk experts identified risks which will become a critical threat to the world. Two of the top five risks which will become critical in the next two years are environmental. All of the top five risks which will become critical in the next five to ten years are environmental.
- We will also be reviewing other reports from risk expert organisations to identify any gaps on our corporate risk register.
- We are working in a new way with workstream leads to identify the areas of our organisation where specific risks would have the biggest impact. This will help us target mitigating actions more effectively.

4. Current risk register and changes during the past year

4.1 Risks that have been realised

A number of risks have been realised this year as a result of COVID-19 and the cyber-attack. These are:

- R012: We fail to comply with environmental and business legislation applicable to SEPA.
- R031: Inadvertent disclosure of sensitive data to internal or external parties.
- R037: SEPA loses networks or data access through insufficient application of Cyber Security and Resilience procedures

Following the cyber-attack, we initially reported that R033: Insufficient Grant in Aid and charging income is available to SEPA to deliver the outcomes committed to in the Corporate Plan 2017-

2022, had also been realised. However, the Scottish Government gave us authority to spend more than our budget in last year's exceptional circumstances, to ensure we could meet our costs. As we recovered our financial reporting systems, it became clear that, with careful management of our spending, we were able to manage within our existing budget and did not need to overspend

4.2 Risks added to the corporate register

R042: SEPA is unaware of levels of non-compliance in registered controlled reservoirs.

This risk is connected to loss of access to information following the cyber-attack.

4.3 Risks being considered for corporate register

Throughout the year staff discuss potential risks with us and we work with them to profile the risks. This process usually provides reassurance that the risks are being managed appropriately and in the right place and it often leads to good discussions about further mitigating action that could be taken.

Areas that we are considering include: incident response; resource challenges; succession planning; information rights response; health and safety documentation; and supply chain disruption in relation to services, staff and equipment.

4.4 Risks removed from the corporate register

- R033a: SEPA overspends against the Scottish Government budget allocation in year and actual costs of delivering services under charging schemes are greater than the fee income generated under the charging schemes.

This risk was removed following the financial year end 2020-2021 as it was a specific risk raised in relation to that year. Following the cyber attack, we initially reported this risk as realised. However once our financial reporting systems were recovered, we discovered this was not the case. This risk is related to R033 explained in section 4.1 above.

- R038: The impact of the UK leaving the EU impacts our ability to deliver against our statutory purpose and actions and targets set out in our corporate plan and Annual Operating Plan.

The overall risk score has been reduced to meet the target score. When this risk was identified it was based on the impact that a no deal EU exit would have on SEPA's ability to deliver our work. Since then, the UK has formally left the EU and the EU-UK Trade and Co-operation Agreement has been signed.