SETA

Deliverable 8.3

Risk Management Plan

Authors
Soo Vinnicombe   s.m.vinnicombe@sheffield.ac.uk

Internal Reviewer
Lucy Moffatt   l.moffatt@sheffield.ac.uk

State: Final
Distribution: Public

Deliverable History

Date	Author	Changes
16 March 2016	Soo Vinnicombe	Initial version
17 March 2016	Sam Chapman	Minor changes to detail further legal compliance and privacy aspects undertaken in the project.
29 March 2016	Soo Vinnicombe	Final version

Contents

1.   Summary

The following document provides detail on the project management means to handle risk and make contingency plans around those risks. The document includes a risk register detailing project risks and mitigation strategies. This document clearly helps to manage and facilitate the delivery of the project goals.

This risk management plan covers both internally and externally induced risks. The risk management plan will be constantly updated, e.g. unforeseen issues with the performance of distributed graph databases develop. Internal risks are related to individual participants: staff may suffer from illness, leave the institution, or change responsibilities within the team. To this end, the plan will cover actions and activities that will enable the consortium to continue its work, e.g. by transferring responsibilities between participants. External risks may arise e.g. changes in data usage regulations. To this end, adjustments of the overall project goals might be necessary and will be agreed with appropriate stakeholders.

2.   Glossary of Terms

Annex I	Otherwise known as the DoW
CA	Consortium Agreement
DoW	Description of Work
GA	Grant Agreement
WP	Work Package

3.   Abstract

SETA is a very ambitious project that requires integration of expertise and data from different communities – research, municipal, and private. Special attention will be paid to a number of potential problems that may affect the outcomes of the project and these problems will have contingency measures in place where possible.

The project coordinator, supported by the project manager, will be in charge of monitoring the risks and will, where necessary, inform the project steering group about specific situations and potential mitigation measures.

There are risks inherent to the project but also there are risks related to the external environment.

4.   Risk and Contingency Plans

A number of risks arise from the objectives set by the proposal. Every attempt has been made to minimise such risks from the outset by recruiting partners into the consortium who have the required skills and knowledge in their particular field of expertise. Moreover, the project has been designed with a sensible and manageable structure that allows for a stepwise approach to achieving the project's objectives.

The specific risks are presented in the following tables and each is presented with a strategy for mitigating and controlling the risk.

4.1.   Agreement risks

Description of risk	WPs	Risk	Impact
Consortium partners cannot agree because of different interests.	All	Low	Severe
Risk-mitigation measures			
The project management foresees clear conflict resolution and decision procedures to resolve this quickly.			

4.2.   Expertise risks

Description of risk	WPs	Risk	Impact
Departure of key experts.	All	Low	Severe
Risk-mitigation measures			
Replacement will be done with a different expert, preferably from same partner, otherwise from a different partner.			
Description of risk	WPs	Risk	Impact
Departure of key partner.	All	Low	Severe
Risk-mitigation measures			
When possible any leaving partner would be replaced with an existing partner. If impossible a new external partner will be sought. In case a departing partner is a case study owner, it is very unlikely that a replacement will be possible, unless this happens very early in the project. In this case the case study will be removed and we will concentrate on the remaining ones.			

We believe we will still be able to produce excellent results as each of the cases provides in itself the required environment to test and exploit the SETA solutions.

4.3. Technological risks

Description of risk	WPs	Risk	Impact
A coherent data ecosystem is not feasible	1-8	Low	Low/ Medium
Risk-mitigation measures			
SETA implements a concept of data and service ecosystem. An ecosystem is per se composite, with parts of different quality and always evolving. The technological ecosystem per excellence – the World Wide Web – is the most obvious example. More than a risk, incoherence is a certainty. We will try to maximise its coherence as much as possible, and we will adopt measures and technologies able to cope with the nature of a constantly evolving environment. An example of these methods is given in the section on excellence when measures for correcting input from crowdsourced sensing are described.			
Description of risk	**WPs**	**Risk**	**Impact**
The project objectives are too ambitious	1-6	Medium	Medium
Risk-mitigation measures			
The project is very ambitious and the possibility that some of its parts do not deliver the full vision is always present. The development timeline is designed in two cycles with intermediate evaluation in order to quickly identify any criticality and to take corrective actions before the final delivery. All wps will aim at delivering a base technology at high TRL designated to provide a baseline guaranteeing the basic information flow among the different architectural components, while at the same time working at lower TRL levels on highly innovative methodologies which will reach maturity towards the end of the project.			
Description of risk	**WPs**	**Risk**	**Impact**
Security of the environment	4-8	Medium	High
Risk-mitigation measures			
The security of the ecosystem is of paramount importance as it will contain information about people whereabouts (e.g. via phones' GPS data), plans and even usual routes. This is why we have a partner (AIZ) in the consortium who specializes in security of information system and solutions and an expert in large scale architectures (SMI) who will oversees the architectural choices and will follow international security standard and will perform an audit before the deployment of the technology.			

4.4. Privacy risks

Description of risk	WPs	Risk	Impact
The technology will have access to sensitive data which could in principle constitute a risk to privacy of individuals	1-8	Medium	High
Risk-mitigation measures			
We will establish guidelines at the beginning of the project and we will make sure that all regulations in terms of privacy are abided to. All applications having access to personal data will have privacy-by-default built in and all data will be anonymised prior to release. Random-generated identifier (typically 256-bit encryption) will be associated to users all data will be encrypted on phones or other devices the users will use to access information. Information on servers will be anonymised and protected according to the most stringent industry standards.			
Description of risk	**WPs**	**Risk**	**Impact**
New laws on privacy prevent collection of specific data	1,2,3	Low	High
Risk-mitigation measures			
The immediate effect would be that some social sensors will become unavailable. For compensation, two options exist: If it is an isolated case (e.g. one specific type of sensors), we			

will investigate and try to adapt the sensing or crowdsourcing strategy so to adapt to the new legislation. If that is not possible, we will look for further methods. We will adjust our plans to comply with the all new regulations.

4.5.   Take up risks

Description of risk	WPs	Risk	Impact
The technology is not accepted by the citizens or business	1,2,3	Low	High
Risk-mitigation measures			
The consortium is well aware of how important that user take up is for the program. If this does not happen, the project will fail its main objectives. This is why we we are working with city councils who have the possibility to reach thousands of citizens and business as institutions (Turin, Birmingham, Santander) and have an established community sense and direct communication with the representations of all categories of users. A careful campaign of diffusion of the message will be devised during deployment to make sure take up happens in large numbers and the ecosystem and associated solutions are used. Services will be tailored to citizens and business needs with a careful program of user centred design based on requirement collected during the first part of the project. The risk of no user acceptance is therefore low as we will involve users in the requirements analysis as well as in informal evaluations throughout the development phases, so that crucial flaws leading to no user acceptance at all should be identified and eliminated early.			
Description of risk	WPs	Risk	Impact
The technology is not accepted by the decision makers	1	Low	High
Risk-mitigation measures			
Decision makers are involved since day 1 in the requirement analysis process and user centred design will make sure that every solution developed will actually fit their needs. Moreover, a typical issue with acceptance of new solutions is the lack of integration with existing legacy systems. The SETA solution will be designed with this in mind. AIZ – who is leading the design activity – are experts solution providers to decision makers with dozens of millions worth of projects in this areas.			

4.6.   Milestone Risks

Description of risk	WPs	Risk	Impact
The deployment is delayed	1	Low	Low
Risk-mitigation measures			
SETA has the very ambitious plan to deploy technology within 15 months. The deployment will be staggered over the third year and at different times in the different cases so to make sure that a smooth take up happens. If technical or social issue delay the deployment by some weeks (or even months) this will not be a major issue as the deployment span is very long and we will be able to perform the project tasks as required.			

4.7.   Ethical Risks

Ethical risks and mitigation will be further addressed in the Privacy Impact Assessment deliverable (D6.1).

Risk	Solution or Mitigation Strategy
Personal Information must be collected and stored according to national legislations.	All partners are committed to do so. For example, the UK Data providers for SETA (e.g. The Floow) are registered with the UK Information Commissioner and conform to the required legislation for handling personal data

	and sensitive information.
	All Data providers will fully adhere to EU and national (e.g. United Kingdom) legislation. This includes but is not limited to:
	• 95/46/EC Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
	• Data Protection Act 1998 (DPA)
	• General Data Protection Regulation 2012 (GDPR)
	• Freedom of Information Act 2000 (FOIA)
	• Computer Misuse Act 1990
	• Regulation of Investigatory Powers Act 2000 (RIPA)
	• Privacy and Electronic Communications (EC Directive) Regulations 2003
	Universities have an additional level of ethical assurance. For example, The University of Sheffield researchers have an obligation to ensure that their research is conducted ethically and with the minimum possible risk to all those involved or affected by it. To this extent the University has put in place a procedure called "ethic research review" that oversees any activity that uses personal data or human participants. The University has also publicly available policy documents that specify consent, confidentiality and data protection etc. (all available at (http://www.shef.ac.uk/ris/other/gov-ethics/ethicspolicy). SETA will strictly adhere to confidentiality and data protection legislation.
Real-life and simulation evaluations will require collection of personal data from volunteers.	In order to carry out tests and evaluations, the project will collect a database of willing participants. When participants will be required for an evaluation, the database of volunteers will be analysed to find suitable participants and the volunteers will be contacted to check whether they are still willing to take part. In case of positive answers, they will be marked as participants. When distributing questionnaires for the evaluation, the questionnaires will be anonymous. The volunteers will have the right to be anonymous for any aspect of the evaluations. Volunteers will be given an anonymous identifier. During evaluation, all participants will be provided with an information sheet that will explain what type of activities will be carried out, what will be the participant's role and what are the alternatives, risks, and benefits for participation in a way easy to understand. Volunteers will be informed of exactly what type of recording of their actions/answers will be performed and that they can decide to withdraw from the experiment at any time and request to view/cancel their data. Wherever possible, participant will be provided with two copies of an "informed consent form" to be signed and dated by the named researcher and freely signed by the volunteer. One copy will be kept by the researcher and the other copy will be given to the participant for their records. The Evaluation Information Sheet and Informed Consent Form will be created for each evaluation following the templates available at http://www.shef.ac.uk/polopoly_fs/1.89756!/file/Consent-Form.doc http://www.shef.ac.uk/polopoly_fs/1.89755!/file/Information-

	Sheet.pdf. For users that will be recruited non in person (e.g. citizens that will download a mobility app), information will be provided both on the SETA website and special detailed permission (e.g. geolocalisation) will be requested via the standard Android or iOS methodologies.
Personal Information will be electronically stored and could be attacked and accessed for malevolent aims	Data access control strategies will provide safeguards on data provided across the consortium. The UK Data providers for SETA (The Floow) have strict Information Security Policies (that can be made available) these comply with ISO 27001 and ISO 27002. Personal Information and information not in the public domain is stored using encryption techniques compliant with the Data Protection Act 1998, General Data Protection Regulation 2012 and the Regulation of Investigatory Powers Act 2000. Secure transmission protocols are in place to protect Remote connections. The Floow has specific procedures for handling of sensitive data; this type of data is stored in a secure area where limited staff have access only via fob, security code or equivalent to gain access. CCTV operates throughout secure zones.
Sensitive personal Information about driving information may be made public	The Flow has full right to the usage and analysis of the information collected from end user drivers. Users of the services have agreed to the terms and conditions of their service, that include the possibility for The Floow to process, analyse and share the data anonymously. To preserve users' privacy The Floow will distribute to the consortium only information that has been anonymised or aggregated for project use to ensure end user level protection.
Personal Information may be released in publications	No publications written using data from the project will mention participants by name/username/personal details or sensitive journey endpoints. Any photo will be anonymised accordingly.
Personal data shared on Social Media may be withdrawn from Social Media	The SETA Social Media Access is carried out through official Public APIs that fully conform with the social media providers terms and conditions of service. For example in case someone who made their profile public changes his mind and makes it private, Twitter will prevent access to data after notification.
Dual Use Implications	Whilst the aims of SETA are to support mobility planning and effective decision-making, we recognise the type of information collected and analysis performed could be misused and could negatively affect society as a whole, if they were improperly disseminated. To this extent SETA has established an external assessor that will examine the project and identify risks related to possible dual-use and suggest solutions or mitigation strategies. The Ethics Advisor will also comment on the dissemination and communication strategy of the project to ensure that the results of the research are disseminated in a responsible way, and not cause any harm. The advisor will

	report to the European Commission on this matter at month 18 and month 36. SETA partners, including public authorities, are committed to not use the collected information or the research results to interfere in the private life of a person unless this is necessary for national security or public safety. In such a case, SETA will comply with the duty of having to alert public authorities to the ethical and practical implications of the research results. SETA will carefully monitor the "dual use" implications of the research results in the yearly PIA.

5. Conclusion

As with all complex projects, SETA presents risks. The original work plan and the project organisation has been designed to explicitly minimise these risks. The steering committee will constantly look out for any changes to risk status but also for emerging risks. The tables above with be revised during the project lifetime to reflect significant changes in the project landscape.