Ref. Ares(2023)7353888 - 28/10/2023

Co-funded by the European Union

SIEMBIOT Risk Management

Ref: expw-2023-208

The following document contains the initial risk register and risk management process for the SIEMBIOT project number 101127939

Release Certificate

Status of this Document:	**Final**
Document Version:	**1.1**
Release Date:	**84 Oct 2023**

Document Control

Title:	SIEMBIOT Risk Management
Customer:	**Internal**
Owner:	**Expertware SRL,** Bd. 1 Decembrie 1918 nr.8, Suceava, Romania VAT: RO19130788
Release Date:	24 Oct 2023
Author:	Andreea Galbau
Total Pages:	10
Security Class:	Commercially Confidential
Distribution:	Customer only
Disclaimer:	The controlled copy of this document is maintained by the author. This document is uncontrolled when printed and should be checked for currency and validity with the author.

Document Approval

Approved By:	Lelcu Ion Didel	Approved by e-mail

Revision History

Version	Date	Issued By	Status	Comments
0.1	9/09/2023	Andreea Galbau	Draft	Initial document
0.2	10/10/2023	Andreea Galbau	Draft	With input from project teams
0.3	21/10/2023	Lelcu Ion Didel	Draft	Updated risk log
1.0	24/10/2023	Andreea Galbau	Final	Final review
1.1	28/10/2023	Andreea Galbau	Final	Updated reference number and TOC

Table of Contents

1 Introduction 4
1.1 Project Description 4
2 Risk Assessment Methodology 4
2.1 Risk Management Team 5
2.2 Risk Reporting, Tracking and Closeout 5
2.3 Criteria for risk identification and assessment 5
6 Risk register 8
2.4 Baseline risk log 8
2.5 Calendar of updates 10
2.6 Document repository 10

1 INTRODUCTION

Risks anticipated for the Modular, open, research platform integrating SIEM, NOC, SOC, CTI and Vulnerability Management (SIEMBIOT) project will be managed using a tailored approach in accordance with the methodology embraced by the aviation industry. The SIEMBIOT Risk Management Plan (RMP) identifies the scope of the project's risk definition and delineates the methodology that has been used to identify, quantify, and assess risks. The level of treatment is graded based on the level of risk determined. The RMP identifies the controls and processes used to identify and mitigate areas of cost, scope, schedule, and technical risk that may occur during project planning and implementation. The RMP will be maintained and updated throughout the life of the project.

1.1 Project Description

The project scope includes the SIEMBIOT platform, which is a modular, open, research platform integrating SIEM, NOC, SOC, CTI and Vulnerability Management. The platform uses an integrated mix of open-source and commercial software tools meant to improve the security posture for the organizations onboarded.

The project leverages other EU research projects (ENISA cyber security PANDORA, Cyber-Trust, others, MISP, OpenCTI) noted in Description of the action (DoA) — Annex 1 (DEP): V1.0 – 01.11.2021 from Project: 101127939 —SIEMBIOT — DIGITAL-ECCC-2022-CYBER-03.

2 RISK ASSESSMENT METHODOLOGY

To ensure a strong quality control system Expertware and DNSC will apply and follow the project risk management approach defined by the PM² methodology of the Commission, complemented with key Prince2 elements. The risk management approach defines the risk control and escalation process as part of the overall project governance structure as well as the structure of the Risk Log which will be used to document and communicate the related risks and the relevant risk response actions.

Risk management brings visibility to risks, accountability as to how they are acted upon, and ensures that project risks are proactively dealt with and are regularly monitored. The main objectives of project risk management are to:

- Identify, address, categorise, approve and report project risks throughout the project.
- Report all major risks to the steering layer of the project (i.e. the Commission, HADEA, the Advisory Board);
- Ensure risk response strategies are in line with project stakeholders' risk appetite and approved risk level thresholds.
- Ensure all risks are monitored and under control.
- Risk response actions are implemented effectively.

The risk management process is divided into the following key steps:

- Step1: Risk identification
- Step 2: Risk assessment
- Step 3: Risk response development
- Step 4: Risk control

The SIEMBIOT Project Managers have overall responsibility for implementing the RMP during the design, construction, and operations phases. However, the SIEMBIOT Risk Management Team will develop and document an organized, comprehensive, and flexible strategy, as well as methods for identifying, tracking and mitigating risk areas.

2.1 Risk Management Team

The SIEMBIOT Risk Management Team performs continuous risk identification and analysis with input from SIEMBIOT engineering and technical divisions. Risk identification is based on teams' experience with similar projects, lessons learned from previous projects, knowledgeable personnel input, and feedback from partners. The risks are analysed, and mitigation actions identified, developed and documented.

The risk assessment is performed continuously, documented monthly and mitigation actions agreed during project board meeting.

Risk management responsibilities will be owned by the SIEMBIOT project managers who will trace day to day progress and actions and will record eventual changes in the risk log.

Risk Management Team

Full name	Role	Company
Lelcu Ioan Didel	Project Manager - Lead	Expertware
Andree Galbau	Project Manager	Expertware
Alina Vasilescu (TBC)	Project Manager	DNSC

2.2 Risk Reporting, Tracking and Closeout

Risk reporting involves documenting risk identification, risk quantification, risk handling strategies, impact determination, and risk closeout.

Risk tracking includes monitoring action items from risk handling strategies/responses, identifying a need to evaluate new risks, and reevaluating changes to previous risks.

Risk closeout represents the steps to assign risk associated action items to a responsible individual and identifying a completion date. Completion dates are tracked, and each action item status updated until closeout.

2.3 Criteria for risk identification and assessment

2.3.1 Classification based on occurrence likelihood

- Very Likely (VL): risk is likely to occur with a probability greater than or equal to 90%.

- Likely (L): risk is likely to occur with a probability greater than or equal to 50%
- Unlikely (U): There is a less than 50% chance that this event will occur.

2.3.2 Classification based on consequence.

Consequence will identify impact that occurrence of this event will have on cost, schedule and/or technical performance of the facility/equipment. Each issue will be evaluated on these three.

	Negligible (1)	Marginal (2)	Moderate (3)	High (4)
Costs	<=€50k	€50 – €100K	€100K - €200K	>€200K
Schedule	None	<20 days	20 - 30 days	>20 days
Quality	None	Minor	Significant degradation	CD-4b will not be met.

2.3.3 Risks quantification

The risk register will use colour coding to mark the priority of actions as the product between the likelihood to happen and the impact generated. This approach is similar with the methodology embraced by the aviation industry.

Likelihood	Impact			
	1 Negligible	2 Marginal	3 Moderate	4 High
4 High	4	8	12	16
3 Likely	3	6	9	12
2 Low	2	4	6	8
1 Not likely	1	2	3	4

2.3.4 Actions based on priorities

Low	Medium	High	Critical
1-3	4-8	9-12	16
Handled during monthly project board meetings	Handled during monthly project board meetings	Request exceptional project board meeting	Request exceptional project board meeting

Project Management team will ensure that any changes in likelihood and impact are updated on time and if need is project board meetings are requested.

2.3.5 **Notifications based on priorities**

Low	Medium	High	Critical
Update risk register	Update risk register Inform owners	Update risk register Inform owners Notify project board	Update risk register Inform owners Notify project board

The notifications will be done via multiple channels: emails, teams sites & channels.

In case of lack of response from the owners, escalations will be triggered to their line managers and the project board.

6 RISK REGISTER

This section presents the results of the specific risk assessments that were conducted for each of the identified project areas of consideration.

2.4 Baseline risk log

Category	Risk Identification	L[1]	I[2]	R[3]	Responsible	Strategy	Counter measure	RR[4]
Personal	Time pressure	2	1	2	Team leaders	Avoidance	Allocate more resources.	90%
	Under skilled risk	1	1	1	Team leaders	Avoidance	Training/Control	90%
	Key resources unavailability	1	2	2	Project team	Mitigation	Ensure backup for each key competence	75%
Financial	Inflation impact on costs	2	2	4	Financial dept	Mitigation	Ensure additional funding reserves are available.	90%
	Energy cost increase	2	2	4	Operational dept|	Avoidance	Ensure energy efficiency for all equipment purchased.	75%
Operational	Equipment acquisition delays	3	4	12	Project Manager	Mitigation	Engage multiple suppliers ensuring that short delivery is enforced in the contracts.	50%
	Unavailability of specific hardware components	2	2	4	Project Manager	Mitigation	Eliminate dependency on a specific component or vendor	95%
	Open-source software components move to commercials	1	3	3	Operational dept	Mitigation	Keep and update software repositories so project can continue using the last open-source release	95%
	Missing project deadlines	2	2	4	Project Manager	Avoidance	Ensure regular reviews and allocate additional resources to meet deadlines.	60%

Category	Risk Identification	L[1]	I[2]	R[3]	Responsible	Strategy	Counter measure	RR[4]
	Deliverables to not pass quality validation requiring rework	1	4	4	Project Manager	Avoidance	For critical phases provision contingency intervals to cater for unexpected issues.	75%
	IT failure – data loss	1	4	4	Operational dept	Avoidance	Embrace IT designs without single point of failure. Ensure daily backups are taken.	95%
	Cyber attacks	2	3	6	Operational dept	Mitigation	Ensure SIEMBIOT platform is protected using multiple cyber security layers.	75%
Strategic	Difficulty to onboard sufficient devices	2	3	6	Project Board	Avoidance	Ensure early promotion, multiple awareness information sessions and participation to cyber conferences.	50%
	Reduce volume of research data	1	3	3	Operational dept	Mitigation	Onboard additional devices to increase the volumes.	70%
	Low engagement from other research partners	3	3	9	Project Board	Mitigation	Allocate more resources for partner engagement and initiate multiple training sessions.	70%
Political	Russia – Ukraine conflict spill to Romania	1	4	4	Project Board	Accept	-	-

L[1] = Like hood degree.

I[2] = Impact.

R[3] = Risk degree.

RR[4] = Response Readiness.

Risks with RR = 100% will be considered closed and moved to a risk closure table.

2.5 Calendar of updates

Risk register will be updated monthly, and project board will be informed during quarterly meetings unless a critical risk emerged.

For traceability & analytics the Risk Management team will save a named copy of the risk log every 6 months.

This approach will ensure that we can compared the baseline risks with actual risks updated during the project execution.

2.6 Document repository

The risk log and the successive updates will be kept in the project management restricted site created on Expertware's Intranet.

https://expertware.sharepoint.com/:f:/r/sites/SIEMBIOT/Shared%20Documents/ProjectManagement/RiskRegister?csf=1&web=1&e=ImA7gJ