|  |  |
| --- | --- |
|  |  |
| A logo with a shield and text  Description automatically generated | |
| CyFORT: Word Template | |
| Quarto reference template 2024  (ALab-CyFORT-QuartoTempl-202407) | |
| This word document is to be used as a custom reference file by the ALab C5-DEC CAD DocEngine publishing tool based on Quarto, i.e., if you wish to produce a docx from your Quarto source files.  This reference file is to be copied into the root of your Quarto project. | |
|  | |

General information

|  |  |
| --- | --- |
| Name of the company | itrust consulting s. à r. l. (ITR)  itrust Abstractions Lab s. à r.l. (ALab)  IAL : ITR + ALab |
| Project title | Cloud Cybersecurity Fortress of Open Resources and Tools for Resilience (CyFORT) |
| Type | Report (REP) |
| Reference | XYZ |
| Version | 1.0 |
| State | Final version |
| Owner | Arash Atashpendar |
| Authors | Arash Atashpendar, Itzel Vazquez Sandoval, Agnese Gini |
| Application date | 16/05/2024 |
| Classification | Restricted |

Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Modifications |
| 1.0 | 03/07/2024 | Arash Atashpendar | Release for July 2024 |

Approval

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Role | Responsibility | Signature |
| A. Atashpendar | CTIO,  ALab | Technical leader,  Project manager |  |
| I. Vazquez Sandoval | R&D Scientist,  ALab | Content agreement |  |
| C. Harpes | Managing Director (MD),  ITR + ALab | Ownership | Or see printed version managed by CISO. |

Management summary

The project status report is used for periodic reporting on the project status, project progress and forecasts as to how the project will proceed. The form and method of reporting are set out in the project management plan. The project takes account of the core organization's specifications regarding reporting content and frequency.

The key dates in terms of project duration based on the official project order are as follows:

* Project start: **17/03/2022**
* Project closure: **30/06/2027**

While each work package of the CyFORT project tackles a rather distinct set of challenges and the creation of dedicated tools, we view the entire set of tools developed within the project as forming a coherent whole, which we refer to as the CyFORT stack of cybersecurity tools. The objectives range from the creation of methodologies, guides and tools aimed at simplifying and enhancing the activities of CERTs/CSIRTs and more broadly, teams operating SOCs, as well as improving secure software development life cycle and cyber-physical system security assessment by building on the Common Criteria and other relevant sources.

Table of Contents

[1 Introduction 5](#_Toc170900720)

[1.1 Context 5](#_Toc170900721)

[1.2 Objectives 5](#_Toc170900722)

[1.3 Scope 5](#_Toc170900723)

[1.4 Enforcement and reading instructions 5](#_Toc170900724)

[1.5 Audience 5](#_Toc170900725)

[1.6 Document structure 5](#_Toc170900726)

[1.7 References 6](#_Toc170900727)

[1.8 Acronyms 6](#_Toc170900728)

[1.9 Glossary 7](#_Toc170900729)

[2 References 8](#_Toc170900730)

List of Figures

**No table of figures entries found.**

List of Tables

[Table 1: Document structure 6](#_Toc170900731)

[Table 2: Acronyms 7](#_Toc170900732)

[Table 3: Glossary 7](#_Toc170900733)

# Introduction

The project status report is used for periodic reporting on the project status, project progress and forecasts as to how the project will proceed. The form and method of reporting are set out in the project management plan. The project takes account of the core organization's specifications regarding reporting content and frequency.

## Context

This document is produced as part of the project management module activities of the CyFORT project [1].

## Objectives

The purpose of this document is to provide regular project status updates, with a focus on used and available resources, deviations from the project plan, risks and revisiting the project outlook.

## Scope

This scope of this document is limited to the CyFORT umbrella project and its subprojects/work packages, namely WP1: IDPS-ESCAPE, WP2: SATRAP-DL, WP3: C5-DEC, WP4: DLT-PSaaS, WP5: CS-GRAM and WP6: PQC-MAT.

## Enforcement and reading instructions

This document will come into effect after approval and distribution to interested parties. It shall be respected and/or formally updated by all active contributors. The use of the SIMPLE PRESENT tense or the terms “MUST”, “MANDATORY”, “REQUIRED”, or “SHALL” in a statement means that the statement is considered a formal requirement. The use of words such as “SHOULD” or the adjective “RECOMMENDED” means that there may be legitimate reasons for disregarding the statement, but that the implications of such an exception shall be assessed and fully understood.

The terminology “MAY” or the adjective “OPTIONAL” means that the implementation of the statement is at the discretion of the implementer. Text marked in red refers to laws or regulations that must be obeyed.

## Audience

This document shall be read and applied by all collaborative parties actively contributing to the project.

## Document structure

The remainder of this document is structured as follows:

|  |  |  |
| --- | --- | --- |
| Section | Title | Description |
| 1 | Introduction | provides a short introduction outlining the purpose, objectives and context of this document. |
| 2 | Overview of project status | Overall status, plus assessments and conclusion |
| 3 | Forecast regarding objective achievement | Forecast with respect to expected system requirements implementation and procedural/process objectives |
| 4 | Target/actual cost comparison and forecasts | Cost/benefit and outlay figures, deadlines and WP outcomes forecast |
| 5 | Problems and measures | Identified problems and suggested measures |
| 6 | Risks | Simplified risk register |
| 7 | Outlook | Next steps |
| 8 | Bibliography | provides bibliographic references. |

Table 1: Document structure

## References

See Section 2 for a detailed bibliography listing books, articles, and reports. Links pointing to resources available online are stored as footnotes on the page containing the first occurrence of such links.

## Acronyms

The table below describes acronyms specific to this document; for a complete list of acronyms, we refer the reader to the project-wide acronym list [2].

|  |  |
| --- | --- |
| Acronym | Explanation |
| ASVS | Application Security Verification Standard |
| AD | Anomaly Detection/Detector |
| AI | Artificial Intelligence |
| C5-DEC | Common Criteria for Cybersecurity, Cryptography, Clouds – Design Evaluation and Certification |
| CC | Common Criteria |
| CMU | Carnegie Mellon University |
| CS-GRAM | Cloud services: Governance, Risk management, Audit, Monitoring |
| CyFORT | Cloud Cybersecurity Fortress of Open Resources and Tools for Resilience |
| DLT | Distributed Ledger Technology |
| DLT-PSaaS | Distributed Ledger Technology – Pseudonymization as a Service |
| DoD | Definition of Done |
| ECSS | European Cooperation for Space Standardization |
| ESA | European Space Agency |
| FID | First Industrial Deployment |
| HR | Human Resource |
| ICT | Information and Communication Technology |
| IDPS-ESCAPE | Intrusion Detection and Prevention Systems for Evading Supply Chain Attacks and Post-compromise Effects |
| ISDP | Information Security and Data Protection |
| ISMS | Information Security Management System |
| KB | Knowledge Base |
| ML | Machine Learning |
| NFR | Non-Functional Requirements |
| NIDS | Network Intrusion Detection System |
| OWASP | Open Web Application Security Project |
| PIM | Platform Independent Model |
| PM | Project Management |
| PMP | Project Management Plan |
| PQC-MAT | Post-Quantum Cryptography Migration Assistance Tool |
| RDI | Research, Development and Innovation |
| RID | Review Item Discrepancy |
| SAMM | Software Assurance Maturity Model |
| SATRAP-DL | Semi-Automated Threat Reconnaissance and Analysis Powered by Description Logics |
| SDLC | Software Development Life Cycle |
| SDPM | Software Development Plan Model |
| SDPM | Software Development Plan Model |
| SEI | Software Engineering Institute |
| SOAR | Security Orchestration, Automation and Response |
| SSA | Software Security Assurance |
| SSAPM | Secure Software Assurance Plan Model |
| SSDLC | Secure SDLC |
| SVVM | Software Verification and Validation Model |
| TM | Threat Modelling |
| TPI | Test Plan Item |
| TRL | Technology Readiness Levels |
| WBS | Work Breakdown Structure |

Table 2: Acronyms

## Glossary

The table below provides a glossary specific to this document; for a complete project-wide glossary, we refer the reader to the corresponding file [2] or versions superseding it.

|  |  |
| --- | --- |
| Term | Meaning |
| CLAUSEN | A consortium of Luxembourgish companies put together to enhance the collaboration, efficiency and effectiveness of SOC and CERT teams across Europe by virtue of new innovative tools and services developed within the IPCEI-CIS. |
| CSIRT | A Computer Security Incident Response Team (CSIRT) is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. Their services are usually performed for a defined constituency that could be a parent entity such as a corporate, governmental, or educational organization; a region or country; a research network; or a paid client. |
| DevSecOps | DevSecOps—short for development, security, and operations—automates the integration of security at every phase of the software development lifecycle, from initial design through integration, testing, deployment, and software delivery. It is the practice of integrating security testing at every stage of the software development process. |
| IPCEI | IPCEIs may represent a very important contribution to economic growth, jobs and competitiveness for the Union industry and economy. IPCEIs make it possible to bring together knowledge, expertise, financial resources, and economic actors throughout the Union. |
| Linter | Linting highlights syntactical and stylistic problems in source code, which often helps you identify and correct subtle programming errors or unconventional coding practices that can lead to errors |
| Review Item Discrepancy | An issue, identified by a reviewer, that is not compliant with a requirement, a review objective, or a design goal. |
| Technology Readiness Level | Technology Readiness Levels are a method for estimating the maturity of technologies. TRLs enable consistent and uniform discussions of technical maturity across different types of technology. |

Table 3: Glossary

# References

|  |  |
| --- | --- |
| [1] | A. Atashpendar, "R050\_PMD\_CyFORT-ProjectDescr\_v1.0". |
| [2] | A. Atashpendar, "R007\_Glossary". |
| [3] | Arash Atashpendar, "C5-DEC Secure Software Development Life Cycle (SSDLC)," itrust Abstractions Lab and itrust consulting, 2023. |
| [4] | Arash Atashpendar, "C5-DEC System Concept," itrust Abstractions Lab and itrust consulting, 2023. |
| [5] | A. Atashpendar, "R005\_CyFORT-MeetActDec". |
| [6] | Arash Atashpendar, "Software Verification and Validation Model (SVVM)," itrust Abstractions Lab and itrust consulting, 2023. |