Ref. Ares(2026)9341274 - 02/10/2026

OSCRAT

Open-Source Cyber Resilience Act Tools

D1.5

OSCRAT Deliverable 1.5 Project Updates

Submission date: 30.09.2026

Author: PMF Research

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.
The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Project acronym	OSCRAT
Project title	Open-Source Cyber Resilience Act Tools
Project Number	01190180
Deliverable Number & Name	D1.5 Project Updates
Work package	WP 1 Project Management
Due Date	31.05.2026 (in the Portal)
Submission Date	30.09.2026
Lead Partner	PMF Research
Version	1.0
Status	Final
Type:	☐ R – Document, Report ☒ DEC – Websites, patent filings, videos, etc. ☐ DEM – Demonstrator, pilot, prototype ☐ Other
Dissemination level:	☒ PU – Public ☐ SEN - Sensitive

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Document History			
Version	**Date**	**Modified by**	**Comments**
0.1	23/09/2026	PMF Research	First Draft
0.2	30/09/2026	PMF Research	Final version

Abstract

D1.5 – Project Updates documents how project information was regularly shared, discussed and made traceable throughout OSCRAT, both within the consortium and, where appropriate, through channels addressed to external stakeholders and the open-source community. In line with the Description of the Action, project updates were supported by an integrated internal collaboration environment based on OpenProject and Nextcloud, complemented by regular governance and coordination meetings, as well as by external communication channels including the OSCRAT website, News and Events sections, newsletters, press releases, public deliverables, training and workshop resources, YouTube, the public GitHub repository and the final OSCRAT platform. The deliverable focuses on the transparency, traceability and continuity of project information rather than duplicating the detailed monitoring analysis of D1.3 or the dissemination-performance assessment of D5.4.

Keywords

OSCRAT; project updates; transparency; OpenProject; Nextcloud; wiki; news; forum; project monitoring; Cyber Resilience Act; open source; stakeholder communication

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

DISCLAIMER

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Table of contents

Executive Summary 5
1. Introduction 6
1.1 Purpose and scope 6
1.2 Position of D1.5 within WP1 6
1.3 Relationship with WP5 communication and dissemination 7
2. Project update framework 8
2.1 Internal project management and governance updates 9
2.2 Public and open-source update environment 11
3. Internal project updates and traceability 12
3.1 Responsibilities, activities and progress updates 12
3.2 Wiki, News, Forum and notifications 13
3.3 Risks, issues and follow-up 13
3.4 Technical development updates 14
4. Public project updates 14
4.1 Website, News and milestone communication 15
4.2 Training, workshops and audiovisual updates 15
4.3 Beta phase and stakeholder feedback 15
4.4 Open-source and technical-result visibility 16
4.5 Final-stage project updates and access to results 16
5. Evolution of project updates throughout OSCRAT 16
6. Conclusion 18

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Executive Summary

Deliverable *D1.5 – Project Updates* documents how project information was regularly shared, discussed and made traceable throughout OSCRAT, both within the consortium and, where appropriate, through channels addressed to external stakeholders. In line with Task T1.6 and the Description of the Action, it focuses on the mechanisms used to communicate project status, progress, responsibilities, issues, decisions and results over the course of implementation.

Internally, OpenProject and Nextcloud provided the shared environment for tracking Work Packages, tasks, deliverables, milestones and supporting documentation, complemented by News, Forum, wiki and notification functions. These tools worked together with monthly consortium meetings, Work Package meetings, TPMs, Steering Committee meetings and exchanges with the Project Officer to keep the consortium aligned on progress, issues and next steps.

Externally, selected communication channels also contributed to the project-update function. The OSCRAT website, News, LinkedIn, YouTube, public deliverables, training and workshop resources and the GitHub repository made significant milestones and results visible to SMEs, the open-source community and the wider CRA ecosystem. Their communication reach and performance are reported separately under WP5.

The final phase marked the transition from development and validation to a complete and publicly accessible result. The official platform launch on 11 September 2026, followed by the OSCRAT in Action demonstration, communicated the availability of the final platform and supporting resources.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

1. Introduction

1.1 Purpose and scope

WP1 – Project Management provides the organisational framework for the OSCRAT project. Alongside tasks and deliverables covering project planning, communication-channel establishment, progress monitoring and stakeholder engagement, deliverable *D1.5 – Project Updates* focuses specifically on how project-status information was shared across the consortium and, where appropriate, communicated to external stakeholders.

D1.5 is closely connected to, but distinct from, other OSCRAT reporting activities. Deliverable *D1.3 – Monitor Progress* explains how project implementation was monitored, including progress against deliverables, milestones, KPIs and risks. Deliverable *D1.4 – Stakeholder Engagement* provides the detailed account of how stakeholders were involved throughout the project. WP5 communication and dissemination activities, and in particular *D5.4 – Dissemination Results*, address how OSCRAT activities and results were communicated to external target audiences and assess the related outputs, reach and performance.

Against this background, D1.5 has a specific and complementary role: it documents the mechanisms through which implementation information was turned into regular project updates, ensuring that partners and governance bodies remained informed about project status, responsibilities, risks, issues, decisions and upcoming priorities, while significant developments were also made visible, where appropriate, to the open-source community and the wider CRA stakeholder ecosystem.

1.2 Position of D1.5 within WP1

The Description of the Action places D1.5 within WP1, under the responsibility of PMF Research, and defines it as a public DEC-type deliverable. Task T1.6 requires the consortium to provide regular updates to project stakeholders, including sponsors, the Steering Committee and project team members, on project *status, risks and issues. The formal deliverable description further specifies that "online transparent responsibilities and tracking of project progress updates are achieved by keeping partners and the open-source community up to date through wiki, news and forum"* channels.

In OSCRAT, these requirements were addressed through a combination of internal project-management and governance mechanisms and stakeholder update channels.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Description of activity	Implementation in OSCRAT
Regular status updates	Monthly consortium meetings, WP meetings, TPMs, Steering Committee meetings, internal reporting and digital project-management updates.
Risks and issues	WP1 monitoring, governance meetings, issue discussions, corrective actions and follow-up.
Transparent responsibilities	OpenProject work packages, tasks, deliverables, milestones, assignees, schedules and progress fields.
Wiki / news / forum	OpenProject wiki/knowledge base, News section, discussion/forum functions and email notifications.
Open-source community updates	OSCRAT website, public News and Events pages, public deliverables and resources, GitHub repository, OSCRAT platform and technical documentation.

Table: Project updates and implementation in OSCRAT

This combination reflects the two dimensions foreseen in the Description of the Action: keeping the consortium and governance bodies regularly informed about implementation, while also providing appropriate visibility of significant project developments and results to the wider OSCRAT and open-source community.

1.3 Relationship with WP5 communication and dissemination

The external communication dimension of D1.5 naturally overlaps with WP5, since some of the same project developments were also communicated through OSCRAT's communication channels. The distinction lies primarily in the purpose for which those outputs are considered.

Within D1.5, communication beyond the consortium is relevant where it demonstrates that a significant project development, milestone, release or result was made visible to OSCRAT stakeholders. WP5, by contrast, addresses the broader communication and dissemination function of those same channels, including their use to raise awareness, engage target audiences, disseminate results and support uptake.

A single project development may therefore contribute evidence to both work packages without serving the same reporting function. For example, the

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

completion of a platform-development milestone may first be communicated internally during a consortium or Work Package meeting as part of the D1.5 project-update process and subsequently be presented externally through the OSCRAT website, a newsletter, LinkedIn or another WP5 communication channel.

For this reason, D1.5 refers to external communication outputs only where they evidence transparent project updates to the open-source community or the wider OSCRAT stakeholder ecosystem. Detailed communication statistics, audience reach and dissemination performance remain within the scope of WP5 and are reported in *D5.4 – Dissemination Results*.

2. Project update framework

OSCRAT relied on a combination of complementary channels rather than on a single mechanism for communicating project updates. Internal project-management and governance channels provided the primary framework for sharing information on project implementation, ensuring operational transparency, traceability of responsibilities and follow-up of agreed actions. Public channels complemented this internal framework by making significant milestones, releases and results visible beyond the consortium, particularly to SMEs, the primary OSCRAT target group, to the open-source community and the wider CRA stakeholder ecosystem.

While these public channels also formed part of the broader communication and dissemination activities implemented under WP5, within D1.5 they are considered only where they provide evidence that relevant project developments were communicated transparently to external stakeholders.

Layer	Main channels	Primary audience	Update purpose
Internal project management and governance layer	OpenProject, Nextcloud, email notifications, consortium meetings, WP meetings, TPMs, Steering Committee meetings, Project Officer interactions	Consortium partners, WP leaders, project management, Steering Committee, granting authority representatives	Track and review responsibilities, activities, deadlines, deliverables, risks, issues, decisions, corrective actions and overall project progress.
Public/open-source update layer	OSCRAT website, News section, public deliverables, OSCRAT platform, GitHub/public repository, selected WP5 communication channels	Open-source community and wider OSCRAT stakeholders	Make significant project milestones, releases and results visible beyond the consortium. Communication reach and performance are assessed under WP5.

Table: Channels for Project Updates, Audience and Purpose

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

2.1 Internal project management and governance updates

OSCRAT's internal project-update framework combined digital collaboration tools with regular governance and coordination exchanges. D1.2 established OpenProject and Nextcloud as the central collaboration environment for the project, hosted on the UNICIS.Tech intranet infrastructure. **OpenProject was** configured as the **main project-management tool,** supporting task tracking, Agile workflows, scheduling, meeting agendas and minutes, wiki and repository functions, structured reporting, as well as discussion and forum functions for project-related exchanges. **Nextcloud** complemented this environment by **providing secure document sharing, real-time collaboration, encrypted storage and version control.**

Together, these tools created a **shared working environment** in which project-status information could be directly connected to the relevant supporting documentation and discussed among project partners where needed.

OpenProject reflected the structure of the OSCRAT work plan through Work Packages, Tasks, Deliverables and Milestones, allowing partners to follow responsibilities, priorities, progress and relationships between activities. Files, repository references, meeting notes and other records could be linked to the corresponding project items, while the discussion and forum functions supported exchanges on specific activities, issues and updates. This helped ensure that project information remained both traceable and accessible to the relevant partners throughout implementation.

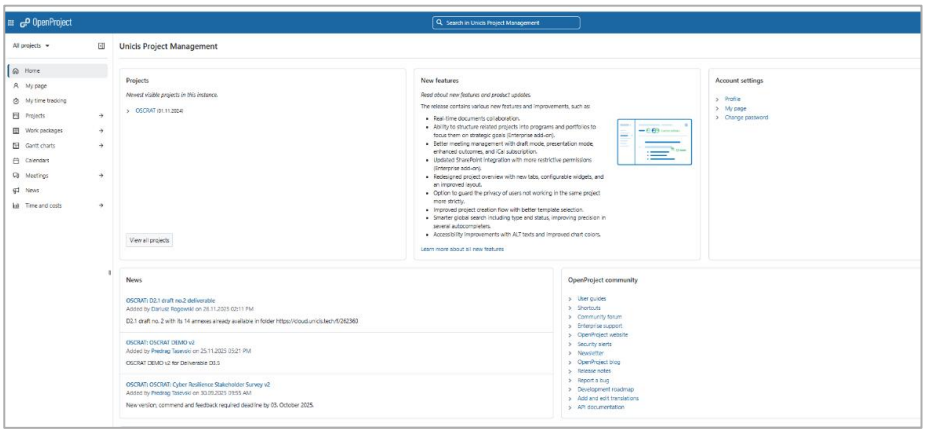


Figure: Open Project Environment

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

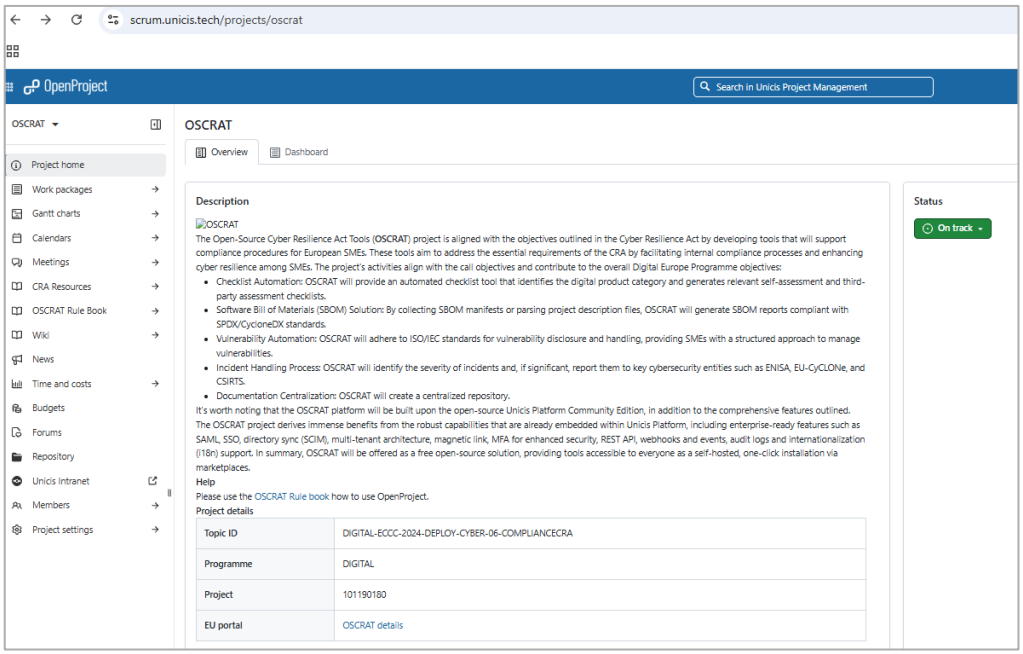


Figure: Open Project Environment

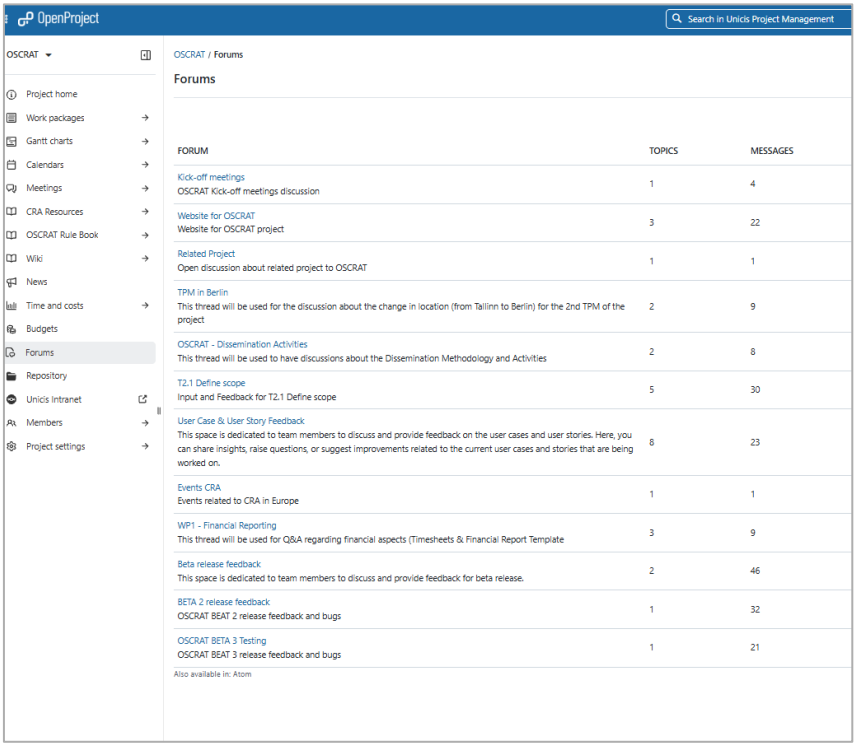


Figure: Open Project – Forum

This digital project-management environment was complemented by the regular coordination and governance meetings foreseen within OSCRAT, which provided the main occasions for sharing and discussing project updates across

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

the consortium. The monthly consortium meetings were used to review progress across the project, follow upcoming deadlines and coordinate activities between the different Work Packages. Work Package meetings provided the space for more detailed technical and operational updates, while the Transnational Project Meetings enabled partners to take stock of implementation progress, discuss interdependencies between activities and agree on the next steps for the project.

Steering Committee meetings provided the forum for discussing matters of strategic relevance and for supporting decision-making on significant implementation issues, including the project-duration amendment. Interactions with the Project Officer offered an additional channel for communicating and clarifying relevant project-management matters and, where necessary, validating proposed approaches.

These exchanges complemented the monitoring activities reported in *D1.3 – Monitor Progress*. While D1.3 explains how OSCRAT followed progress, deliverables, milestones, risks and corrective actions, D1.5 focuses on how this information was regularly shared with partners and governance bodies, keeping the consortium aligned on project status, decisions and next steps.

2.2 Public and open-source update environment

The public update layer complemented OSCRAT's internal project-management and governance framework by making important project developments visible to external stakeholders. It centred mainly on the **OSCRAT website** and, particularly in the final stages of implementation, on the project's public open-source environment.

Over the course of the project, the OSCRAT website was the main public reference point for project updates and results. Through the News section, public deliverables, event information and project resources, external stakeholders could follow key stages in OSCRAT's development and the progressive availability of its outputs. This was particularly relevant for SMEs, as OSCRAT's primary target group, as well as for cybersecurity actors, the open-source community and the wider CRA stakeholder ecosystem.

The **public GitHub repository** adds a specific open-source dimension to this environment. It provides public access to the OSCRAT source code and technical result, complementing the information available through the website and supporting transparency, reuse and further development of the platform.

OSCRAT's LinkedIn channel also supported the public update function by amplifying selected project milestones, including project activities, training and workshop opportunities, platform-development updates and the final launch of the OSCRAT platform on 11 September 2026. Within D1.5, LinkedIn is considered

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

only where it helped communicate the state of play or availability of OSCRAT results; its reach and engagement performance are reported under WP5.

The **OSCRAT YouTube channel** provided an additional public-access point for project-related content. Recordings of the four training sessions, four thematic workshops and the Final Launch Event were published on the channel, allowing stakeholders who had not participated live to access the content afterwards. These recordings also documented the progressive presentation of OSCRAT's approach, platform functionalities and final results. Their dissemination performance remains within the scope of WP5.

The **stakeholder engagement activities** implemented under WP4 also contributed to the project-update function. Beyond their main knowledge-sharing and training purpose, the training and workshop programme progressively connected CRA requirements with the evolving OSCRAT platform. In particular, the workshops provided opportunities to present and demonstrate platform functionalities and to show stakeholders how the project was translating regulatory requirements into practical workflows.

The **beta release** represented a further stage in this process. It formed part of the 2026 validation and refinement phase, during which feedback from project reviews and product demonstrations was used to support further bug fixing and improvement before the final release.

Other WP5 communication outputs, including **newsletters, press releases and public events,** also communicated selected OSCRAT milestones. For D1.5, these are relevant only where they document significant developments in project implementation, platform maturity, releases or final results. Their broader communication reach and performance are reported separately under WP5, particularly in *D5.4 Dissemination Results*.

3. Internal project updates and traceability

3.1 Responsibilities, activities and progress updates

The internal update process followed the structure of the OSCRAT work plan. Work Packages, tasks, deliverables and milestones were represented in OpenProject and linked to the partners responsible for their implementation. This allowed the consortium to maintain a shared view of ongoing activities, upcoming deadlines and dependencies between different parts of the project.

Partners regularly provided updates on the activities under their responsibility, including completed work, work in progress, deliverable preparation, upcoming actions and any issues requiring coordination. PMF Research, as Coordinator and WP1 leader, used these inputs together with the information available in

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

OpenProject and the project meetings to maintain an overall view of implementation.

Supporting material could be linked directly to the corresponding activity, including working documents, meeting notes, repository references and deliverable files. Nextcloud complemented this process by providing the shared document environment and version control used by the consortium.

The detailed monitoring methodology and status of deliverables, milestones, KPIs and risks are reported in *D1.3 – Monitor Progress***.** In D1.5, these elements are considered from the perspective of how the resulting information was made available and communicated across the consortium.

3.2 Wiki, News, Forum and notifications

The functionalities established under D1.2 directly supported the specific D1.5 requirement to keep partners updated through wiki, news and forum channels.

Within OpenProject, the **News** function was used to publish information relevant to the consortium, while the **Forum and discussion functions** allowed partners to exchange feedback and discuss specific project topics. The project wiki/knowledge-base functions provided a persistent space for project information that could be consulted independently of scheduled meetings.

The Forum was also used for exchanges linked to concrete OSCRAT activities, including meeting discussions, dissemination activities, stakeholder feedback, beta-release feedback and testing. This gave partners an additional asynchronous channel for commenting on activities and sharing information between formal coordination meetings.

Email notifications complemented these functions by alerting users to relevant changes and updates within the project-management environment.

Together, these tools ensured that project information did not depend solely on scheduled meetings or individual email exchanges but remained available within a shared environment that partners could consult throughout implementation.

3.3 Risks, issues and follow-up

Project updates also covered important implementation issues and changes, in line with Task T1.6. When technical, organisational, regulatory or timing-related matters arose, they were discussed through the appropriate Work Package, consortium or governance channels and followed up through the project-management process.

A relevant example was the extension of the OSCRAT implementation period. The need for additional time was first discussed within the project governance

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

structure, including the monthly consortium meeting and a dedicated Steering Committee meeting, and subsequently with the Project Officer before the consortium formally requested a four-month extension. The approved amendment extended the project to 30 September 2026. For D1.5, this process illustrates how a significant change affecting project implementation was communicated, discussed and translated into an agreed project-wide update.

3.4 Technical development updates

Technical development generated a substantial part of the project-status information exchanged throughout OSCRAT. Progress was communicated through the requirements work carried out in WP2, where the stakeholder survey also served as an important consultation mechanism with the project's target groups, as well as through the successive WP3 testing cycles, product releases and the preparation of the final User Manual and technical documentation.

The testing reports prepared at different stages of implementation provided recurring reference points for the consortium, showing which platform functionalities had been completed, which were still under development and which required further testing or refinement. By the final development stage, the OSCRAT platform had reached feature-complete status and incorporated the main functionalities developed across WP2 and WP3, including compliance assessment, SBOM and scanning functions, vulnerability and incident management, documentation management, configuration management, risk assessment, the technical documentation checklist, security-awareness functions and expanded audit logging.

These technical updates supported consortium coordination and informed subsequent testing, training, demonstrations and the preparation of the final public release.

4. Public project updates

As described in Section 1.1, OSCRAT's public communication channels are considered in D1.5 where they were used to communicate concrete developments in the project, including progress in platform development, testing and validation phases, demonstrations involving stakeholders, releases and the final availability of project results. The detailed inventory, reach and performance of communication and dissemination activities are reported separately in *D5.4 – Dissemination Results*.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

4.1 Website, News and milestone communication

The OSCRAT website provided the main public reference point for following the development of the project. Over the course of implementation, the website was progressively updated to reflect OSCRAT's evolution from project set-up and requirements gathering to platform development, validation and final release.

The News section communicated key project developments, including progress in implementation, stakeholder activities, training and workshop phases, platform-development milestones, beta-related updates and, ultimately, the official launch of the final OSCRAT platform.

Newsletters, press releases and LinkedIn posts also amplified selected milestones to external stakeholders. Within D1.5, these channels are relevant where they communicated changes in project status, progress in platform maturity, upcoming phases or the availability of results. Their audience reach and engagement performance remain within the scope of WP5.

4.2 Training, workshops and audiovisual updates

The **WP4 training and workshop programme** provided important opportunities to update stakeholders on the development of OSCRAT. While these activities primarily served training and stakeholder-engagement purposes, they progressively linked CRA requirements with the evolving platform and, in several cases, included practical demonstrations of OSCRAT functionalities.

The **OSCRAT YouTube channel** extended access to these activities beyond the live sessions. Recordings of the four training sessions, four thematic workshops and the Final Launch Event were made available online, allowing stakeholders to revisit both the CRA-related content and the way the OSCRAT platform and its functionalities evolved over the course of the project.

For D1.5, these activities are relevant where they helped communicate the state of play of the project, the development of the platform or the availability of new results. Participation figures, audiovisual output counts and dissemination performance are reported separately under WP5.

4.3 Beta phase and stakeholder feedback

The beta release represented an important transition from development to validation and refinement. During this phase, the platform was subject to further internal review, product demonstrations and technical validation activities, including penetration testing. The resulting feedback and findings contributed to bug fixing, security improvements and further refinement ahead of the final release.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

This phase therefore marked a clear change in project status, with OSCRAT moving from development towards broader validation, testing and refinement of the platform in preparation for the final release.

4.4 Open-source and technical-result visibility

The **public GitHub repository** provides public access to the OSCRAT source code and related technical results, complementing the information available through the project website and technical documentation. In this way, it supports transparency towards the open-source community and enables the reuse, further development and potential adaptation of the OSCRAT platform beyond the end of the project.

4.5 Final-stage project updates and access to results

During the final project phase, public updates increasingly focused on the availability and usability of the completed OSCRAT results.

The OSCRAT website and Resources section brought together the final OSCRAT platform, the CRA Applicability Check, public deliverables, the User Manual, full product documentation, use cases and best practices, as well as the training and workshop materials.

The ***official platform launch on 11 September 2026*** and the subsequent *OSCRAT in Action* demonstration marked the closing stage of this update process. At that point, external communication shifted from reporting work in progress to informing stakeholders that the platform and its supporting resources were complete and available for use.

This represented the final stage of the project-update process: OSCRAT had progressed from requirements gathering and development, through testing and validation, to a publicly accessible, documented and operational result.

Looking beyond the end of the project, these final updates also supports the sustainability of OSCRAT. The next step is to continue promoting the OSCRAT platform and its resources to stakeholders, particularly SMEs, and to encourage continued registration and use of the platform. Maintaining access to the website, documentation, training materials, public repository and platform will help ensure that the results remain visible, reusable and available to organisations preparing for CRA compliance beyond the project lifetime.

5. Evolution of project updates throughout OSCRAT

The content of project updates evolved together with the project itself. During the first months, updates focused mainly on setting up the project-

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

management environment, defining responsibilities and establishing the technical and organisational basis for implementation. As OSCRAT moved into requirements definition and platform development, updates increasingly concerned technical progress, testing and dependencies between Work Packages. The final months shifted towards validation, completion of the platform, the public release and access to the final results.

Period	Main project phase	Main focus of updates
Dec 2024 – Feb 2025	Project set-up	Kick-off, Project Plan, collaboration environment, allocation of responsibilities, first technical activities and initial public project information.
Mar – Aug 2025	Requirements and early development	WP2 requirements gathering, stakeholder inputs, initial WP3 development and testing, coordination between technical partners and first public progress updates.
Sep – Dec 2025	Requirements consolidation and testing	Finalisation of D2.1, successive testing activities, CRA training sessions, stakeholder engagement updates and communication of the transition towards platform development and beta activities.
Jan – May 2026	Beta development and validation	Beta-stage development, thematic workshops, platform demonstrations, stakeholder feedback, M15 testing, public updates through website, newsletters and LinkedIn, and preparation for the final development phase.
Jun – Sep 2026	Final development, release and closure	M18 testing, completion of platform functionalities, User Manual and full documentation, public GitHub repository, final resources, YouTube recordings, official platform launch, Final Event and OSCRAT in Action demonstration.

Table: Main update phases

This progression also reflects the changing balance between internal and public updates. The earlier stages required more intensive coordination within the consortium, while the later stages increasingly combined internal project updates with communication of completed results to external stakeholders. Pasted text

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

6. Conclusion

Throughout OSCRAT, project updates were integrated into the day-to-day management of the action. OpenProject and Nextcloud supported continuous access to project information, while consortium, Work Package, TPM and Steering Committee meetings ensured that progress, issues, decisions and upcoming actions were regularly discussed with the relevant partners.

As the project evolved, the content of updates moved from project set-up and requirements gathering to technical development, testing, beta validation and finally the release of the completed platform. Selected external channels complemented this process by communicating significant milestones and making results accessible beyond the consortium.

The final launch of the OSCRAT platform and the availability of the website, documentation, training resources, public repository and supporting materials also provide the basis for continued visibility, reuse and promotion of OSCRAT beyond the funded project period.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

OSCRAT

Open-Source Cyber Resilience Act Tools

OSCRAT – D1.5 Project Updates

www.oscrat.eu

https://www.linkedin.com/company/oscrat-eu-project

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.