Secure Code Audit - Order-to-Payment (gerard.frankowski@man.poznan.pl)

1. Who is the main point of contact for service ordering? □

Whom and how should customer contact in order to activate the service?

Task Leader (TL) or Activity Leader (AL). Customer contacts via email

2. Is there a service user identification process? □

What is the process to decide if the service user is entitled to service - who and how is doing that?

No formal process but it should be mentioned in the request that the software is implemented in particular project activity and thus eligible for the service. Then the preassessment survey is in place where activity and task must be provided. In problematic cases TL or AL may be involved to make a decision.

3. What kind of data is requested and collected from the customer/service user? □

(e.g. Service user names, service user organization, etc.) How is data collected (Forms, applications, etc.)?

General data about the service (especially if SCA is a part of a general review) – in the preassessment survey:

https://wiki.geant.org/display/gn41sa4/Pre-assessment+survey

Technical data – see https://wiki.geant.org/display/gn41sa4/Input+to+the+security+audit

4. How is the availability and/or feasibility of the service determined for a particular customer/service user? □

e.g. If there are any customized service offerings to the service user or if the service is a part of the standard offering?

SCA is a part of more general validation service. The SCA is a part of a standard offering. But the standard offer is tailored to the customer demands (e.g. SCA may be done only for specific part of the software, or emphasis may be put on particular class of security vulnerabilities)

5. How is the availability of resources needed to support the service determined? □

e.g. availability of computer hardware, servers or network resources, etc.

The basic resource is available manpower. The necessary effort is based on information gained from the customer (see Question 3) – mainly size of the source code for manual analysis is important. The farthest possible deadline is also taken into account, if necessary. After effort estimation it is determined if sufficient resources are available by the deadline date. If not, different actions may be taken like refusing the service (least preferred), asking for additional manpower from AL, proposing less thorough tests which will take less effort

6. Is there any kind of customer/user subscription inventory used in the process? □

e.g. Database with detailed information about customers and services provided to them?

There is no subscription inventory used in the process of SCA itself, but there is an internal repository at the level of SA4T1 task, where information about request and their statuses are handled (including SCA).

7. Is there a need to contact the service user during the order completion phase? If yes, who is doing that and how? □

e.g. If service user participates in commissioning or end-to-end testing during service setup phase.

Yes, the TL/SM interacts with users to get necessary information (e.g. software source code and documentation), access to the testbed and other information which are needed to start the service.

8. Is there a person in charge of issuing a Service order and how is that being done? □

e.g. The person who checks that all requirements are met, the customer request can be fulfilled, and then issues an order to implement the service.

AL or TL verify all preconditions are met (both from the side of the customer and the SM) and the TL initiates starting the SCA – via email or by assigning tasks in JIRA.

9. Is there a person in charge of issuing a Resource order and how is that being done?

If the service requires special resources that need to be provisioned (e.g. hardware, switches, servers, etc.) this would be the person initiating the process to obtain them.

In general such an order is necessary only if extra resources are necessary (see Question 10)

10. What if adequate resources are missing (e.g. servers, network equipment, etc.)? Is there a person in charge of supply, allocation and installation of needed resources?

How are new resources configured and tested? Describe that process.

The critical resource is manpower. If it is lacking, or an expert with particular skill is not available (e.g. when the code is written in a programming language that current experts know little) , TL and if necessary AL, may apply to reassign expert from another task or assuring manpower for an external expert.

11. Is there a person in charge of closing Resource order?

When acquiring new resources, this would be the person who confirms that all needed resources are obtained and set up. Describe this process briefly.

There is no formal process for Resource ordering in terms of manpower. It is rather determined before the assignment of new resources that if they will be acquired, they will be sufficient to complete the SCA.

12. Is there a need to allocate specific service parameters during the service setup phase? How is that data recorded?

E.g. service parameters like service identifiers, IP addresses, domains, VLAN IDs, etc. This data could be recorded using database, forms, paper, etc.

In general, there are no specific technical parameters connected with the audit. Data collected from customer during the planning phase are the basic input. In particular cases there may be collected e.g. single IP addresses (e.g. the testbed address).

The acquired data are collected in the internal Wiki

13. Briefly explain implementation, configuration and activation of the service. □

E.g. persons or teams involved and their tasks.

It is described in the details here:
https://intranet.geant.org/gn4/1/Activities/SA4/_layouts/15/WopiFrame.aspx?sourcedoc=/gn4/1/Activities/SA4/Deliverables%20Documents/Service%20Validation%20and%20Testing%20Process/D8-1_Service-validation-and-testing-process.docx&action=default
(Deliverable 8.1) in the chapters 4.2.3 Security code audits.

14. How is the service tested before it is activated for the service user, and by whom? □

E.g. end-to-end testing to confirm that service is working according to agreed performance levels.

N/A

15. Is there a person in charge of closing Service order? □

E.g. Confirmation that service is configured and working as expected.

SM/TL closes the service order internally (when the final report is ready to be delivered to customer).
TL closes the service order (customer gets the report and accepts the results)

16. Is there a person who monitors that service user provisioning activities are assigned, managed and tracked efficiently to meet the agreed committed availability date? □

E.g. Someone who is responsible for tracking whether service activation is going as planned.

This is TL responsibility

17. How (and by whom) is service user being contacted after service is activated? □

E.g. the person who contacts the service user by email, phone call, etc.

All team members may contact the customer and vice versa usually by email exchange or with regular and ad-hoc remote communication forms (skype, VCs, Web conferences, etc.).

18. Is there a person or team in charge of closing the service user order? □

E.g. After the service is activated, a person who is providing closing or management report.

N/A

19. How is service user satisfaction being validated? □

E.g. Survey to check if the delivered service meets service user expectations.

Currently there is no formal method, but the user may (and often does) send his comments and questions to the report, usually also expressing a general opinion about the service.