**Developing Skill Standards for OSS Compliance**

OpenChain Japan WG

Promotion Subgroup OSS Skill Standards Development Team

(Masato Endo / Ayumi Watanabe / Tomo Dote / Yukiko Kamijo / Mitsutoshi Yamada)

1. Background

In recent years, with the increase in scale and complexity of systems, it has become difficult for even international tech giants to develop software on their own. And the development of various products with open source software created by an open community (hereinafter referred to as “OSS”) is increasing. In addition, with the progress of IoT, companies that have hardly dealt with software in the past have come to use OSS. Under such circumstances, "work that builds an in-house process that can appropriately fulfill the OSS license conditions and allows engineers to participate in and contribute to the OSS community", that is, "OSS license compliance work" (hereinafter referred to as "this work"). This work is attracting attention of companies for maintaining their technical capabilities and acquiring human resources by making appropriate and maximum use of OSS. We, the OSS Skill Standards Development Team, have highlighted the importance of OSS utilization by companies in terms of competitive strategy, and clarified the process of this work, which is an essential and unique work in OSS utilization. Since it is an urgent work for companies to develop and secure human resources who can properly perform the work, we have tried to formulate a skill standards framework.

1. Importance of skill standards development

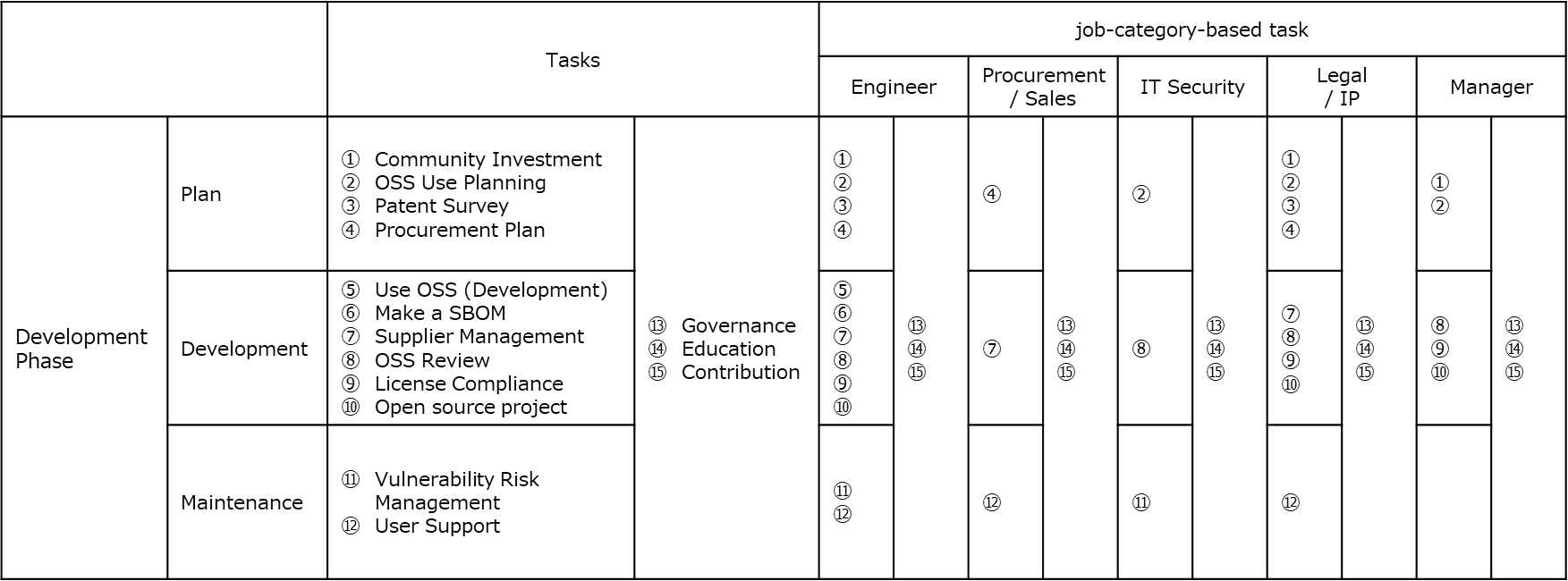
As mentioned above, in addition to the complexity and sophistication of this work, it is necessary for various departments within the company to cooperate to carry out this work, so people need to know appropriately whose responsibility each task is. In addition, since this work is a relatively new work for organizations, it is necessary for organizations’ human resource development to have “skill standards” as an index that clarifies and systematizes the abilities required to carry out this work. As a matter of fact, even in the OpenChain Specification 2.0, which is the global standard of the OSS compliance program by OpenChain Project, it is required to define the role that influences the performance and effect of the program and the responsibility. It is also required to evaluate the competency of the roles and document the results of the evidence of competence evaluation.

However, the specification does not mention specific items or indicators such as what role each department should play and how each person in charge should be evaluated, and it is left to each company. Therefore, it is considered that the necessity of developing "skill standards" is increasing from the viewpoint of the competitive strategy of companies, the strengthening of technological competitiveness, and the acquisition and recruitment of human resources. Here, the "skill standards" is an index that clarifies and systematizes the individual's ability (skill) required to carry out the target work, and the ability is the knowledge required for the work and it means practical ability (achievement / experience). In Japan, we already have some existing skill standards including those for IT, IP human resources, standardized human resources, etc., but in developing the skill standards for this work, the "Standardized Human Resources Skill Standard" (developed by Kazunari Sugimitsu, Yukiko Kamijo, Yushi Komachi, Toshiaki Kurokawa, Mizue Hayashi, published as “Skill standards for assessing the skills required of human resources” in 2013) is considered to be particularly useful as a reference for development. The standardized human resources skill standard clarifies the tasks required for standardization activities, then defines the indicators and skill levels for evaluating the skills required of the personnel who perform those tasks, and finally defines a skill card that defines the skills to be considered for each level. Therefore, in this activity, as the first step in developing skill standards related to this work, we decided to clarify the subdivided work phases required for the execution of this work and created a skill standards framework.

1. Skill Framework and Job-category-based Task

Table 1 below shows the "skill framework and job-category-based task" created by the authors as the first step in developing skill standards. In the left area of Table 1, the vertical axis is the development phase "planning", "development", and "maintenance", and the tasks are described for each phase. As common tasks, 13) Governance, 14) Education and 15) Contribution are listed in the right column. On the other hand, in the right area of Table 1, the horizontal axis is the job category, and the tasks that the person in charge of each job category should perform in each business phase from "planning" to "maintenance" are described.

Table 1: Skill Framework and Job-category-based Task



1. Definition of Job-category-based Tasks
2. Community investment: Consider and implement investing in cost and resources for OSS that are indispensable for promoting the company's business or is a prerequisite for the company's competitive area and industry standard platforms.
3. OSS use plan: Investigate licenses, vulnerabilities, quality, technical barriers, etc., consider OSS and version to be utilized, utilization method, and formulate an OSS utilization plan. Conduct export control-related surveys on the OSS to be used.
4. Patent survey: Investigate the patent risk related to the OSS to be utilized and change the OSS utilization plan as necessary.
5. Procurement plan: When outsourcing software development, make a contract considering a policy on whether or not to utilize OSS and how to utilize it, reporting obligation when utilizing OSS and creation / submission obligation of SBOM (List of utilization OSS: Software Bill of Materials).
6. Use OSS (software development): Based on the OSS utilization plan, acquire the OSS to be utilized from a reliable source in the format most suitable for the purpose of utilization. At that time, consider the existence of licenses and vulnerabilities, and if there is a risk, consider changing the version to be used. If you need the prerequisite software, get them as well.
7. Make a SBOM: Perform appropriate configuration management for the OSS to be used and create SBOM without excess or deficiency of information. Tools may be used to create SBOM.
8. Supplier management: Order part or all of the development work from the supplier based on the procurement contract. Perform an acceptance inspection on the delivered program and confirm that it is not different from the corresponding SBOM. If there is a difference, ask the supplier to correct it.
9. OSS review: Examine the consistency between SBOM and OSS use plan. In particular, the final applicability will be examined and decided from the viewpoint of license security risk and maintenance in the adopted implementation method.
10. License compliance: For all OSSs used, we will fulfill the obligations of each license in order to comply with the terms of the license. Specifically, it includes description of copyright information and preparation for source code disclosure.
11. Open source project: If there is software that should be distribute as an OSS, consider the license to be applied and the publishing method, and implement OSS distribution by an appropriate method.
12. Vulnerability risk management: Collect OSS vulnerability information on a regular basis to detect vulnerabilities that affect the OSS used in products and services at an early stage. If an influential vulnerability is found, the content of the vulnerability, the conditions under which it becomes apparent, the attack method, etc. will be investigated, and triage, repair method and scope of impact will be examined and repaired according to the severity.
13. User support: Create a contact point for inquiries from users regarding OSS used in products and services and respond appropriately to inquiries and requirements.
14. Governance: Clarify the results of examining various matters related to OSS as the organization's OSS policies, rules, and guidelines, and disseminate them within the organization.
15. Education: Educate the organization about OSS policies, rules, guide runs and various rules and procedures.
16. Contribution: Contribute to the OSS community by providing development deliverables, requests, and patches. Contributions include sharing knowledge such as posting articles on technical blogs and presentations at conferences, and user groups and community activities.
17. Future Plan

As a future plan, we are planning to create a detailed map for each task clarified in the skill framework and a skill card corresponding to the job level of the person in charge, aiming to create skill standards related to this task. The skill card will include "business evaluation index" and "competence evaluation index" as skill evaluation indexes for this business.

1. Request for Your Contribution

We would appreciate it if you could give us any feedback and comments. Let us know what you think through GitHub.

If you are interested in the activity, please contact us at the email address below.

Contact us: [oss-skill-standard@googlegroups.com](mailto:oss-skill-standard@googlegroups.com)