Secure Acquisition
Case 4: Supplier Capability Evaluation

January 2020

Case 4: Supplier Capability Evaluation

Using the Supplier Community of Practice content from the Checklist *Capability Maturity Assessment Checklist* outlined in NIST-IR 7622, assess the competency of the organization in the case. You must provide a complete plan as well as the outcome of the assessment (score).

Maturity levels will be assessed using the scale provided across the top of the instrument. For each practice please rate its execution as: Incomplete, Performed, Managed, Predictable, and Optimizing. The various common features of each capability level will help guide your decision in placing your response.

Incomplete: The Incomplete level has no common features. There is general failure to perform the base practices. There are no easily identifiable work products or outputs of the practice.

Performed: Base practices of the process are generally performed. Individuals within the organization recognize that an action should be performed, and there is general agreement that this action is performed when required. The performance of these base practices is ad-hoc and is not rigorously planned, or tracked. Performance depends on individual knowledge and effort. There are identifiable work products for the process Work testify to the performance of the practice.

Managed: The performance of the process is planned and tracked and executed systematically within the organization. Base practices are performed according to a well-defined process using approved methods which are tailored versions of standard, documented processes.

Predictable: Execution of the process is fully reliable because detailed measures of performance are collected and analyzed. This leads to a quantitative understanding of process capability and an improved ability to predict performance. Performance is objectively managed. The quality of work products is quantitatively known.

Optimizing: Quantitative process effectiveness and efficiency goals (targets) for performance are established, based on the business goals and system assurance case of the organization. Continuous process improvement against these goals is enforced by quantitative data that is obtained from the execution of the defined processes as well as from piloting innovative ideas and technologies.

Selection of Appropriate Communities of Practice

The total set of potential practices encompasses the recommendations of NIST IR 7622 "*Supply Chain Risk Management Practices for Federal Information Systems*" (NIST, 2010), which is the most authoritative current reference for proper ICT supply chain risk management practice. The practices in NIST IR 7622 apply differently within three different communities of practice; Acquirers, Suppliers and Integrators. Therefore, depending on the role your organization plays you may be required to fill out this assessment tool for more than one community of practice. And as a consequence, the checklist identifies different assessment items representing each of those notional communities.

How to Do the Assessment

Using the Case, please address each practice in the instrument as an individual, unique requirement. Provide your best estimate of the level of execution for each of these requirements. Depending on your judgment place a [number] "1" in the column that most appropriately describes the level of execution of each of the individual practices.

At the bottom of the instrument you will find a grand-total ranking for the degree of process capability for each of the columns. The sum is the total number of responses for each maturity level. You will be able to roughly determine your organization's level of capability maturity based on where the bulk of your responses fall. This will allow you to judge the relative maturity of your overall supply chain risk management process, as well as the areas where some improvement may be required.