

Secure Acquisition

Case 3: Adequacy of ICT SCRM Practice Assessment

January 2020

Copyright 2020 The University of Detroit Mercy.

NO WARRANTY

THIS UNIVERSITY OF DETROIT MERCY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. THE UNIVERSITY OF DETROIT MERCY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. THE UNIVERSITY OF DETROIT MERCY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this report is not intended in any way to infringe on the rights of the trademark holder.

Internal use. Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

External use. This document may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Case 3: Adequacy of Acquisition Practice

Explanation of the Assessment Process

The purpose of this assignment is to evaluate the current capability maturity of your ICT supply acquisition security practice. The assessment will determine areas in your organization where proper acquisition risk management is being practiced, as well as the relative maturity of those practices. The goal is to generate a nominal ranking of capability maturity based on a universal scale of process performance.

Case

For this case we are addressing Detroit Defense's need to upgrade their F-16F aircraft. Specifically as it pertains to updating the current navigation system with an Advanced Global Positioning System (GPS) capability. For this effort the GPS model chosen for this aircraft has been previously utilized in a similar application for the fire control system for the military's AH64D (Apache Longbow helicopter). Consequently, it is considered to be a Commercial off the Shelf (COTS) application.

Capability Maturity Assessment Checklist -Supplier Community of Practice		Not Done	Performed	Managed	Predictable	Optimized
		0	1	2	3	4
I.	Contractor Name: Wild Blue Yonder Technologies, Inc (WYBT)	3	63	96	0	0
	Role: Sub-Contractor: Updating Current Navigation System with GPS Capability					
II.	Contractor Name: Baseline Defense Technologies, Inc.	0	58	102	0	0
	Role: Sub-Contractor: Updating Current Navigation System with GPS Capability					
III.	Contractor Name: Lafayette Aeronautics	3	53	106	0	0
	Role: Sub-Contractor: Updating Current Navigation System with GPS Capability					
IV.	Contractor Name: Belle Isle Space Administration	8	70	84	0	0
	Role: Sub-Contractor: Updating Current Navigation System with GPS Capability					
V.	Contractor Name: Interlochen Technologies, Inc. (8 (A) Contractor)	2	56	104	0	0
	Role: Sub-Contractor: Updating Current Navigation System with GPS Capability					

Based on the examination and analysis of the summary results using the *Capability Maturity Assessment Checklist* for suppliers, we identified a concern with one of the sub-contractors identified for this effort (Interlochen Technologies, Inc.) The concern relates to the sub-contractor's limited maturity in terms of the number of performance metrics that are not rated as optimized. While this concern exists, the fact that the sub-contractor is an 8 (A) Contractor, with preference provided by Detroit Defense. The Prime Contractor will implement additional contract surveillance controls to ensure that all work efforts performed under the contract along with any respective contract modifications will be met and at a level consistent with the performance requirements established for the work effort.

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*", 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 complete the *Capability Maturity Assessment Checklist* for more than one **community of practice**. And as a consequence, the checklist identifies three different assessment items representing each of those notional communities.

The *Capability Maturity Assessment Checklist* that outlines programmatic activities and general requirements for **acquirers, integrators, and suppliers** can be found starting on page 25 of the NIST IR 7622 document. <https://csrc.nist.gov/publications/detail/nistir/7622/final>

How to Complete the Assessment

Using the Case, please address each practice in the checklist 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. This 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.