Commercial Off The Shelf (COTS) Risk Evaluation Categories

Eric Ferguson, Harry Levinson, Julie Cohen

January 23, 2020

This document is intended to be used by any commercial or government organization that is looking to acquire a commercial off the shelf (COTS) product. It contains risk categories which, based on SEI experience, are always present when purchasing a COTS product. For each category there is a description of the risk along with a recommended risk evaluation criterion. Each criterion should be tailored to the organization's requirements and intended use of the COTS product.

There are five high-level evaluation categories:

- Life-Cycle Requirements Management
- Implementation and Support
- Performance
- Security Risk
- Technology Risk Mitigation

These risk categories, along with the suggested evaluation criteria, can be adapted for use in multiple situations. They include

- defining the requirements for the system to be acquired
- creating selection criteria for selection processes (When used as evaluation criteria, the criteria can be tailored to meet the acquisition strategy and existing organizational policies.)
- tracking risks while the project is executing

The categories and criteria use a few terms that are defined from a COTS solution perspective:

- **Configuration** is built into the COTS product. By changing the configuration, the COTS solution has designed, verified, and will support the performance of the product in all possible combinations of configuration settings. Quite often the number of configuration settings is large, so the COTS solution has a set of configuration tools to enable reliable development and management of the configuration for the COTS solution.
- **Extensions** enable additional capability to be added to the COTS solution. One of the methods for extensions includes an API (application programing interface) that allows for using custom code (plugins, add-ons, scripts, applications, and the like) in a way that never modifies the core application. Using the published APIs means the extensions should continue to work after upgrades of the COTS solution. This custom code can be developed by the COTS solution vendor, third party developers, or in house by the using organization. The API is supported by the COTS solution but the added capability requires full software development techniques to ensure the new capability works as desired.
- **Customization** is the modification of the baseline COTS product via software that is made for a specific customer and not included in the publicly available COTS product.

1. Lifecycle Requirements Management

The risk evaluation categories in this section focus on the ability to effectively scope the COTS solution to obtain the most essential, core features needed by the organization.

1.A. Minimize Modification

The goal of this category is to prioritize configurability over customization. Minimize the extensions and customization to the COTS solution which must be developed to achieve Initial Operational Capability (initial utility). Consider the potential of the COTS solution to support the current range of reports, interfaces, conversions, extensions, and forms/workflows, mostly through configuration rather than customization. A possible source for analysis is the number of extensions/customizations needed to meet the initial and subsequent deliveries.

1.B. Feature Modularity

Consider that the solution allows for incremental acquisition and implementation of desired features through the use of optional features or modules that can be activated and/or purchased at a future date, for use when needed. Review COTS solution for specific statements about modularity, modular architecture, availability of optional features or modules that can be purchased later, etc. You can also compare the COTS solution total numbers of "in base product" versus "extended/customized" features needed for the initial and subsequent deliveries. Quite often for popular products, the feature modules are available from third-party vendors.

2. Implementation and Support

The risk evaluation categories in this section focus on the level of effort and resources required to implement and sustain the COTS solution (e.g., extensibility, number of additional subject matter experts required, and existing federal government contract vehicles).

2.A. Product Maturity

Consider the relative maturity of the proposed COTS solution. This includes the degree to which the proposed solution has been successfully used elsewhere in environments similar to the anticipated use. In addition, consider the total number of years of supporting the proposed solution for other customers.

2.B. Product Widely Used

Consider whether other commercial and government organizations have direct, prior, favorable business experience with the COTS solution. It is best if there has been prior business with other government customers where the COTS solution successfully satisfied its contractual obligations regarding quality, performance, cost, and planned delivery schedule. For example, speak with some of the prior government customers (this may require working through the cognizant government contracting official).

2.C. Extensibility

Consider whether the COTS solution has the ability to easily add new features in the future without breaking any of the existing core or customized software. Review the COTS solution for specific statements about extensibility, extensible architecture, and availability of optional features or modules that can be purchased later. Compare the COTS solution total numbers of "in base product" versus "extensible" features. In addition, refer to statements from the COTS product prior customer references as to the outcomes of managing their extensions.

2.D. Implementation Expertise

Consider whether there is adequate availability of in-house and contractor resources for implementation both initially and for ongoing sustainment. A skills assessment should consider whether the COTS solution will be hosted internally, in the cloud, or as a SaaS (Software as a Service) solution. Also consider the availability of outside expertise capable of using the COTS extension tools and techniques to implement the needed features.

2.E. Operational and Maintainability Expertise

Consider the amount of additional support staff effort required for post-deployment sustainment. This includes both in-house IT/application expertise along with external support from contractors and/or the COTS vendor. Consider the completeness and accessibility of the technical documentation needed to ensure operation and maintenance of the system. Also consider the COTS solution costs and expected range of contract deliverables including testing, training, and administration documents.

3. Performance and Interoperability

The risk evaluation categories in this section focus on the potential to effectively address the performance, usability, availability, and interoperability requirements.

3.A. Performance

Consider if the COTS solution, running on the available hardware and/or other intended hosting infrastructure, is capable of delivering the response time, transaction throughput, and number of users for the first installation. Also consider whether the system will grow to meet future needs. This category should also consider the general usability of the system by the existing users, to include Section 508 (government-wide IT accessibility) requirements, if applicable.

3.B. Robustness

Consider the availability and reliability of the COTS solution. This includes the ability to incorporate new data validation features. Review how the COTS solution responds to error situations, such as data error detection and exception handling.

3.C. System Interoperability

This area considers the COTS solution's support for system interoperability (both internal and *external*). The COTS solution should provide a standard set of methods of interfacing with external enterprise, system, and technical architectures through the use of common standard interfaces.

3.D. Data Interoperability

This area considers the ability of the COTS solution to support new/modified data input or data exchange formats. Review the proposed COTS technical solution for statements like data abstraction, data access layer, data interfaces, "extract, transform, load" (ETL) support, and support for multiple COTS vendor database systems (e.g., Oracle, IBM Db2, MS SQL Server, Postgres, NoSQL databases).

4. Security

The risk evaluation categories in this section focus on the ability to achieve security accreditation.

4.A. Accreditability

It is better if there is minimal or no requirement for introduction of previously unaccredited COTS/GOTS (government off the shelf) infrastructure components that might require extra risk assessments/ validation/approval. For example, is there any "open source" software in the solution which is not already approved by the enterprise?

4.B. Security Vulnerabilities

Evaluate the number of times the COTS solution has been identified with CRITICAL/SEVERE vulnerabilities in the National Vulnerability Database (NVD), hosted by the National Institute of Standards and Technology (NIST). Your organization's cybersecurity team will be familiar with the NVD, and can help you understand the risks concerning COTS weaknesses and vulnerabilities posted on the site. To search the NVD, go to https://web.nvd.nist.gov/view/vuln/search.

5. Technology Risk Mitigation

The risk evaluation categories in this section focus on the ability to keep pace with technological advancements.

5.A. Technical Obsolescence

Determine the degree of reliance on niche and/or immature COTS products in the underlying infrastructure. Review the frequency of updates that deliver new features and the history of inserting new technical innovation. This includes keeping compliant with standards as they are adopted or updated by the cognizant industry and government organizations.

5.B Migration Potential

If you are using a system that is made up of multiple COTS product, consider whether any of the individual COTS products have the potential for to be reused in other capacities if one or more of the associated COTS products is no longer available. Also consider how easy it will be to migrate data and workflows to new products in the future.

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

DM20-0048