SQUARE for Acquisition: Case Study 3

June 2010

This work was funded by

# 

Copyright 2010 Carnegie Mellon University.

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY 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. CARNEGIE MELLON UNIVERSITY 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.

Table of Contents

[Introduction 1](#_Toc265160298)

[The Business Context 2](#_Toc265160299)

[The Acquisition Organization 2](#_Toc265160300)

[Roles and Responsibilities 2](#_Toc265160301)

[Overview of the Process 3](#_Toc265160302)

[The Process Steps 4](#_Toc265160303)

[Step 1 – Agree on Definitions 5](#_Toc265160304)

[Step 2 – Identify Assets and Security Goals 7](#_Toc265160305)

[Step 3 – Identify Preliminary Security Requirements 9](#_Toc265160306)

[Step 4 – Review COTS Software Package Information and Specifications 10](#_Toc265160307)

[Step 5 – Finalize Security Requirements 12](#_Toc265160308)

[Step 6 –Review of Requirements 13](#_Toc265160309)

[Step 7 – Perform Trade-Off Analysis 15](#_Toc265160310)

[Step 8 – Final Product Selection 17](#_Toc265160311)

[References 18](#_Toc265160312)

# Introduction

Using commercial-off-the-shelf (COTS) products is a common practice because it has many benefits. It improves the delivery time of products, results in shared development costs with the customer, and provides an opportunity to enhance capacity and performance of the products.

According to the *A Process for COTS Software Product Evaluation* [Comella-Dorda 2004] and *A Process for Context-Based Technology Evaluation* [Lewis 2005] reports, a COTS product is

* sold, leased, or licensed to the general public
* offered by a vendor for profit
* supported and evolved by the vendor, who retains the intellectual property rights
* available in multiple, identical copies
* used without modifying internals

This document presents a case study on COTS software acquisition for use in a course or workshop. Different organizations have different business goals when they evaluate and choose COTS products. This case study provides guiding steps adapted from the Security Quality Requirements Engineering (SQUARE) process that an acquisition organization liaising with security specialists and COTS vendors can use. These steps should help the acquisition organization make an informed decision about the most appropriate COTS product. This case study also focuses on security and highlights the importance of considering and evaluating security requirements as part of the overall acquisition process.

The audience of this case study is software engineering managers and practitioners who plan to acquire and use COTS products.

# The Business Context

## The Acquisition Organization

The acquisition organization is a growing IT services company that provides banking solutions and software support worldwide. It provides a comprehensive range of financial services, including personal financial services, commercial banking, corporate and investment banking, private banking, and consumer finance, and other related services.

As part of its financial growth and to sustain its growing number of employees, the organization wishes to improve its human resource management systems operations. Currently the company uses legacy systems and a hierarchical database to manage all the company data. It now wants to acquire a relational database management system that would help better manage its data and improve the performance of its operations. The organization is looking for COTS products and will go though the steps in this case study before choosing a final COTS product. This acquisition would help the company better manage their operations, such as

* managing employee payrolls
* maintaining a management information system for employee records
* managing employee skill sets

## Roles and Responsibilities

Workshop participants will adopt the following three primary roles:

* acquisition organization—Participants in this role will represent stakeholders in the organization who will evaluate and choose a database solution from a set of available COTS products.
* COTS vendors—Participants in this role will represent COTS vendors, such as Oracle and MySQL. Their role is to liaise with the acquisition organization and help them in their process of selecting the final product. The vendor would ideally provide support once the product has been acquired and is being deployed. However, that is out of the scope of this case study.
* security specialists—Participants in this role will act as subject matter experts in database security. Because the primary focus in this case study is on choosing a product that meets a set of security requirements, these specialists will help the acquisition organization identify and finalize security requirements for the organization.

# Overview of the Process

The steps adapted from the SQUARE process that will be used for this case study are shown in Figure 1.

Figure 1: Overview of the Process

# The Process Steps

In the remainder of this document are descriptions of each of the eight steps in the SQUARE process for acquiring COTS products, tasks for workshop participants, and samples to help with the tasks. The participants may use some other technique or methodology to complete the steps; the examples are only meant to serve as a guideline.

Table 1 shows a summary of the responsibilities for each of the roles. Additional description of the roles is included in each step.

Table 1: Description of the Roles in the Overall Process

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Step Number** | **Step** | **Acquisition Organization** | **COTS  Vendors** | **Security Specialists** |
| 1 | Agree on definitions | ✓ | 🗶 | ✓ |
| 2 | Identify assets and security goals | ✓ | 🗶 | ✓ |
| 3 | Identify preliminary security requirements | ✓ | 🗶 | ✓ |
| 4 | Review COTS software package information and specifications | ✓ | ✓ | ✓ |
| 5 | Finalize security requirements | ✓ | 🗶 | ✓ |
| 6 | Review security requirements | ✓ | 🗶 | ✓ |
| 7 | Perform trade off analysis | ✓ | 🗶 | ✓ |
| 8 | Final product selection | ✓ | 🗶 | ✓ |

## Step 1 – Agree on Definitions

To establish a common understanding between the different stakeholders of the acquisition organization, the participants of the acquisition organization must agree on a set of definitions to be used throughout this process. The purpose of this step is to ensure that there are no ambiguities in terms and that everyone has the same perspective on these terms. The security specialists can be consulted for input on the terms and definitions.

|  |
| --- |
| **Task**  Participants from the acquisition organization and the security specialists need to collaborate to develop a list of definitions. The exit criterion for this task is a well-documented and agreed-to set of definitions. These definitions will be used throughout the entire process.  Sample definitions and guidance are below.  Time: 20 minutes |

### Sample Definitions

As a starting point, participants can refer to Table 2, which was part of the initial SQUARE case study [Mead 2005, Table 24]. Standard definitions are also available in popular public resources such as IEEE [IEEE 1990], the Software Engineering Book of Knowledge [IEEE 2005], and Wikipedia [Wikipedia 2010].

Table 2: Sample Terms to be Defined

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| access control | access control list | antivirus software | artifact | asset |
| attack | auditing | authentication | availability | back door |
| breach | brute force | buffer overflow | cache cramming | cache poisoning |
| confidentiality | control | corruption | cracker | DoS attack |
| disaster recovery plan | disclosure | disgruntled employee | downtime | disruption |
| encryption | espionage | essential services | exposure | fabrication |
| fault line attacks | fault tolerance | firewall | hacker | honey pot |
| HTTP header manipulation | impact | incident | incident handling | integrity |
| interception | interruption | intrusion | intrusion detection system | intrusion prevention system |
| liability | luring attack | malware | man-in-the-middle attack | masquerade |
| modification | non-essential services | non-repudiation | patch | penetration |
| penetration  testing | physical  security | port scanning | privacy | procedure |
| recognition | recovery | replay attack | resilience | resistance |
| risk | risk assessment | security policy | script kiddies | spoof |
| SQL injection | stakeholder | stealthing | survivability | target |
| threat | threat assessment | threat model | toolkits | Trojan |
| trust | uptime | victim | virus | vulnerability |
| worm |  |  |  |  |

Following are sample definitions that are relevant to the selection of database software.

* encryption—the process of transforming plaintext information to a format unreadable except to those who possess a special knowledge (key)
* brute force protection—the process of providing a means of protecting encrypted data against brute force attacks, for example, attacks that use intelligent strategies to find the correct key to break into a system
* authentication—the process of attempting to verify the digital identity of the sender of a communication, such as a request to log in
* auditing—the information gathering and analysis of assets to ensure that such things as policy compliance and security are protected from vulnerabilities

## Step 2 – Identify Assets and Security Goals

The purpose of this step is for the acquisition organization to agree on a set of assets and security goals for the project. In this step, assets are identified and a high-level business goal is first defined and is then broken down into its constituent security goals. This set of goals is the origin from which the security requirements of the project will be mapped.

|  |
| --- |
| **Task**  Using the information in *The Business Context* section, the acquisition organization and the security specialists will agree on a business goal and then identify assets and prioritize security goals. The exit criteria for this step are a single business goal and several prioritized security goals for the project.  Samples of a business goal, assets, and a set of security goals follow.  Time: 20 minutes |

### Business Goal Example

The database solution should support data security by ensuring no authorized access is possible to the database without prior authentication.

### Sample Assets

* confidential data of all employees
* all relevant database error logs
* database performance tuning results
* list of critical systems being used in the project
* access control rights of all users on high security systems
* security and inspection procedures for using the tools

### Security Goals Example

Figure 2 includes sample goals about database management systems. Note that in this example, confidentiality and availability are security goals, but scalability and performance are not.

Figure 2: Mapping of Goals and Requirements

## Step 3 – Identify Preliminary Security Requirements

The purpose of this step is for the acquisition organization to elaborate on the security goals and develop a list of preliminary security requirements.

|  |
| --- |
| **Task**  This task for the acquisition organization, with assistance from the security specialists, is to brainstorm on the security goals for the project and develop a list of preliminary security requirements. The exit criterion for this task is a set of documented preliminary security requirements.  Time: 20 minutes |

The following set of sample requirements map to the goals in Figure 3, including both the security goals and the additional goals for scalability and performance.

* access control support—The database should provide support for user authentication and network encryption wherever required.
* database location—The database should be able to be placed in an internal network zone to minimize the direct attempts to the database from an un-trusted network.
* database auditing—The database should provide support for recording all the information performed on the database. This information can be used to troubleshoot database availability and performance problems.
* database size—The database should provide support to handle large amounts of data.
* performance tuning—The database should support capabilities that monitor performance and troubleshoot performance issues.

Figure 3: Mapping of Requirements to Goals

## Step 4 – Review COTS Software Package Information and Specifications

This step is to review COTS products, including their package information and their specifications. This step helps the acquisition organization develop an additional set of requirements. This step also introduces the COTS vendors, who will collaborate with the acquisition team and the security specialists and help them review and better understand the specifications of the different products.

|  |
| --- |
| **Task**  This task for all the participants—the acquisition organization, the COTS vendors, and the security specialists—is to review information on all COTS products being considered. The security specialists can provide input on the security features that the products should possess and initiate discussions with the vendors on whether their suite of products addresses the preliminary security requirements developed in Step 3. Samples of database and security features follow in Figure 4 and Figure 5. The exit criterion is a set of documented features and specifications for the COTS products.  Time: 20 minutes |

Figure 4 and Figure 5 are examples of package information and specifications that are typically considered while selecting a database management system. While the information is graphical to show a complete snapshot, the participants must record the information in a proper documented form such as a spreadsheet or document.

Figure 4: Database Features

Figure 5: Security Features

It is best practice to maintain a spreadsheet that documents all the information. An example of such a spreadsheet is in Table 3.

Table 3: Example of Spreadsheet of Database Features and Limitations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name of Database | Fundamental Features | | Limitations | |
| Referential Integrity | Transaction Management | Max Table Size | Max row and columns size |
| Database 1 | <Enter package information> | <Enter package information> | <Enter package information> | <Enter package information> |
| Database 2 | <Enter package information> | <Enter package information> | <Enter package information> | <Enter package information> |

## Step 5 – Finalize Security Requirements

The goal of this step is to finalize the security requirements. Based on the reviews of the COTS packages and discussions with the vendors, the acquisition organization and the security specialists should brainstorm on the requirements and develop a final list of requirements.

|  |
| --- |
| **Task**  This is a task for the acquisition organization and the security specialists. After reviewing the initial requirements and the information contained in the spreadsheet in Table 3, brainstorm and develop a final set of requirements. The exit criterion for this step is a set of finalized security requirements.  The template in Table 4 can be used to document the final set of requirements. The requirements in the template are samples.  Time: 20 minutes |

Table 4: List of Sample Requirements

|  |  |
| --- | --- |
| Requirement # | Requirement Description |
| R1 | The database should be able to be placed in an internal network zone so as to minimize the direct attempts to the database from an un-trusted network. |
| R2 | The database should provide support for user authentication and network encryption wherever required. |
| R3 | The database should provide support for recording all the information performed on the database. This information can be used to troubleshoot database availability and performance problems. |
| R4 | The database should provide support to handle large amounts of data. |
| R5 | The database should support capabilities that monitor performance and troubleshoot performance issues. |

## Step 6 –Review of Requirements

The requirements that are documented in Step 5 should be accurate, quantifiable, and verifiable. In this step, all the requirements are carefully reviewed and changed if necessary.

|  |
| --- |
| **Task**  This is a task for the acquisition organization. After carefully documenting all the requirements, review the requirements to ensure they are accurate and are consistently understood by all the stakeholders without ambiguities. The exit criterion for this step is a reviewed set of final requirements.  Time: 15 minutes |

### Conducting a Formal Inspection

One way to review requirements is to use a formal inspection process like Fagan inspections [Fagan 1976]. Formal inspections offer a systematic way to find and objectively verify defects in documents. As non-executable artifacts, quality requirements can be effectively controlled by a process of formal inspection. The following inspection process is a simplified version of a Fagan inspection, focused towards requirements inspection.

1. Assign Roles

* facilitator—leads the inspection and moderates the meeting
* reader—reads the requirements for all participants
* participants—follow the material that the reader reads and find defects in the requirements
* recorder—records defects found during inspection
* author—answers any questions that participants may have

2. Prepare for Inspection

* The facilitator prepares for an inspection.
* Every member in the meeting individually reviews the requirements and generates an initial list of questions they have and/or defects they find.

3. Conduct Inspection Meeting

* The reader reads one requirement at a time.
* Participants state the defects they find or ask questions.
* The reader reviews each item in the Requirements Inspection Checklist below against the requirements, and the participants agree or disagree about whether the checklist item is passed.
* The writer documents defects found by the team.

4. Revise the Requirements

After the meeting, the author revises the requirements based on the list of defects generated during the inspection meeting.

### Requirements Inspection Checklist

This is the inspection checklist from the Fagan inspection [Fagan 1976]:

1. Are the requirements written correctly and concisely?
2. Are all the requirements written at a consistent and appropriate level of detail?
3. Do the requirements address the concern of the client?
4. Is any necessary information missing?
5. Does any requirement duplicate or conflict with any other requirements?
6. Are all the requirements really requirements and not implementation details? (Remember that requirements concern what, not how.)

It’s a good idea to maintain a record of review comments and defects that arise from the requirements review. Participants can record their comments in the sample review log in Table 5. Documenting review comments can be helpful when requirements of a similar nature originate in the future—the comments from the review log can be analyzed and used as a defect prevention mechanism to ensure that similar defects do not repeat themselves in the future, which will significantly reduce the review time.

Table 5: Sample Review Log

|  |  |  |  |
| --- | --- | --- | --- |
| Requirement Number | Description of Defect | Severity | Suggested Changes |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Step 7 – Perform Trade-Off Analysis

The purpose of this step is to evaluate the COTS products by performing a trade-off analysis on the requirements developed in Step 5 and reviewed (and possibly changed) in Step 6.

|  |
| --- |
| **Task**  This is a task for the acquisition organization and the security specialists. Using evaluation criteria based on the requirements, evaluate the products and develop a prioritized list of COTS products. The exit criterion for this task is a prioritized list of COTS products.  Time: 25 minutes |

Participants may find the following two techniques useful in this step.

### Multi criteria decision analysis

Multi-criteria decision analysis (MCDA) is a process for supporting decision making when there are many evaluation criteria. The overall score is computed by a summation of scores in all criteria [Linkov 2004]. The MCDA process steps are

1. Define the problem.
2. Find all possible risk assessment methods.
3. Generate a set of criteria to be used.
4. Evaluate the feasibility of the criteria, including coverage of all concerns.
5. Create a decision matrix to be used.
6. Add weighting to each criterion.
7. Reach a consensus on the score of each criterion.
8. Compute the score based on each criterion and determine the best weighting

Table 6 provides a template for performing a trade-off analysis of COTS products. We are using a tailored version of the MCDA process. The template includes sample data, but participants should brainstorm to determine their own values in this task. Using the weights in the following scale, the criteria, based on the requirements, are scored according to how effectively the database supports them.

* 3—supports the criteria fully
* 2—supports the criteria but has an operation overhead
* 1—does not support the criteria

Table 6: Template for Evaluating the Products Against the Criteria

| **Criteria** | **Database 1** | **Database 2** | **Database 3** | **Database 4** |
| --- | --- | --- | --- | --- |
| Size | 3 | 1 | 3 | 2 |
| Operational capabilities | 1 | 2 | 1 | 1 |
| Data Type Support | 2 | 2 | 2 | 2 |
| Complexity | 2 | 2 | 1 | 2 |
| Native network Support | 2 | 2 | 1 | 1 |
| Password complexity | 3 | 1 | 2 | 3 |
| Resource Limit | 2 | 3 | 1 | 3 |
| Auditing capabilities | 1 | 1 | 2 | 3 |
| **Final Score** | **18** | **16** | **14** | **20** |

In this example, Database 4 supports most but not all of the criteria; it does not provide a full suite of operational capabilities and native network support compared to the other databases. Performing a trade-off analysis would help the acquisition organization determine the tradeoff between security and performance. In this example, the resource limit requirement is fully supported, which meets the high performance criterion. However, the database does not provide native network support, that is, the solution would compromise on security by allowing network traffic to be transmitted in a non-secure manner. So would you choose Database 4? Or, if security is a more important requirement, would you choose Database 1?

### First Fit Versus Best Fit

Because going through the evaluation process for the entire suite of products can be a tedious and lengthy process, these approaches help you make a decision quickly. The First Fit and Best Fit approaches are defined in the *A Process for COTS Software Product Evaluation* report [Comella-Dorda 2004].

In theFirst Fitapproach, the organization chooses the first product it evaluates that satisfies its needs before choosing an entire suite of products. First Fit considers minimum requirements and answers the question, “Is it good enough?”

Best Fit is similar to the MCDA approach and should be used when there is an appreciable gain in getting more than the minimal amount of some characteristics. Best Fit is also the approach to use in situations where no product has all the capabilities being sought in a particular evaluation. Best Fit answers the question, “How good is it?”

These two approaches will enable the acquisition organization to decide on a product based on the importance of the requirements and the stakeholders’ priorities.

## Step 8 – Final Product Selection

The purpose of this step is to select the final product based on the decisions from Step 7. The decisions should be in line with the business context, the security goals, and the requirements.

|  |
| --- |
| **Task**  This task is for the acquisition organization. Based on the decisions in Step 7 and keeping in mind the overall business objective, make the final selection for the COTS product. The exit criterion for this step is the final COTS product from the list of prioritized COTS products.  Time: 15 minutes |

# References

[Comella-Dorda 2004]

Comella-Dorda, Santiago; Dean, John; Lewis, Grace; Morris, Edwin; Oberndorf, Patricia; & Harper, Erin. *A Process for COTS Software Product Evaluation* (CMU/SEI-2003-TR-017, ESC-TR-2003-017). Software Engineering Institute, Carnegie Mellon University, 2004.

http://www.sei.cmu.edu/library/abstracts/reports/03tr017.cfm

[Fagan 1976]

Fagan, M. E. “Design and Code Inspections to Reduce Errors in Program Development.” *IBM Systems Journal 15*, 3 (September 1976): 182-211.

[IEEE 1990]  
IEEE. *IEEE Standard Glossary of Software Engineering Terminology*

(IEEE Std 610.12-1990). Los Alamitos, CA: IEEE Computer Society Press, 1990.

[IEEE 2005]  
IEEE. *Guide to the Software Engineering Body of Knowledge*. http://www.swebok.org/ (2005).

[Lewis 2005]

Lewis, Grace A. & Wrage, Lutz. *A Process for Context –Based Technology Evaluation* (CMU/SEI-2005-TN-025). Software Engineering Institute, Carnegie Mellon University, 2005.

http://www.sei.cmu.edu/library/abstracts/reports/05tn025.cfm

[Linkov 2004]

Linkov, I.; Varghese, A.; Jamil, S.; Seager, T.P.; Kiker, G.; & Bridges, T. “Multi-Criteria Decision Analysis: A Framework for Structuring Remedial Decisions at Contaminated Sites.” *Comparative Risk Assessment and Environmental Decision Making*, (2004): 15-54.

http://www.environmentalfutures.org/Images/ArmyPaper\_Oct31.pdf

[Mead 2005]

Mead, Nancy R.; Hough, Eric D.; & Stehney II, Theodore R. *Security Quality Requirements Engineering (SQUARE) Methodology* (CMU/SEI-2005-TR-009, ESC-TR-2005-009). Software Engineering Institute, Carnegie Mellon University, 2005.

http://www.sei.cmu.edu/library/abstracts/reports/05tr009.cfm

[Wikipedia 2010]

Wikipedia: The Free Encyclopedia. http://www.wikipedia.org/ (2010).