Contracting out Governmental Web Services

(Externalisation de l'hébergement de sites web gouvernementaux)

Laurent ROGER
DGA/DCE/CELAR
BP7419 35174 Bruz
France

laurent.roger@dga.defense.gouv.fr

ABSTRACT

Contracting out governmental web services

This paper describes the out contracting process of governemental web services focused on the analysis of provider's security measures.

This analysis relies on CELAR (French MoD – Procurement Agency) savoir faire. Input, output, tools and process improvements are described.

The results of the assessments conducted during the past 3 years are pushed into System Security Engineering-Capability Maturity Model. A new concept is proposed ,based on this model : the adaptative confidence profile. Lessons learned are detailed in conclusion.

Externalisation de l'hébergement de sites web gouvernementaux

L'exposé porte sur la démarche d'externalisation de l'hébergement de sites web gouvernementaux en particulier l'examen des dispositions de sécurité des hébergeurs.

L'analyse de ces dispositions est réalisée suivant un savoir-faire maîtrisé par le CELAR (Ministère de la Défense - Délégation Générale pour l'Armement - Centre d'Electronique de l'Armement) depuis 1998. Les éléments clés de ce savoir-faire sont décrits : entrées, sorties, outils et amélioration du processus.

L'évaluation des résultats pratiques obtenus depuis 3 ans est effectuée par rapport aux modèles de maturité SSE/CMM (System Security Engineering-Capability Maturity Model): présentation du modèle SSE/CMM, grille d'analyse pour l'hébergement (profil de confiance dynamique), retour d'expérience.

*Paper presented at the RTO IST Symposium on "Adaptive Defence in Unclassified Networks",
held in Toulouse, France, 19 - 20 April 2004, and published in RTO-MP-IST-041.*

1.0 CONTRACTING INTERNET SERVICES FOR MOD

French Ministry of Defense identified early Internet both as a threat for his information systems and an opportunity for his institutional communication.

The first project was in 1998 the www.defense.gouv.fr web site. Upgrades of this site and other web sites project are now available on Internet : research (www.recherche.dga.defense.gouv.fr) , on line procurement (www.achats.defense.gouv.fr) , armament portal (www.ixarm.com), etc …

Use of internet services is defined by Ministry of Defense directives [1][2][3]. Directives advise the project manager to use CELAR expertise for security aspects.

Basic requirements for those projects are :

- **domain naming** : usually root domain is gouv.fr, exceptions are handled by a committee
- institutional communication requires **integrity** of incoming data (news, publishing time) and output data (web pages). Public image of MoD must be preserved.
- Web sites must be available anywhere, anytime. Stopping for short period of maintenance might be accepted but overall **availability** is a major concern.
- **Imputability** : MoD wants to be sure that unidentified person can't produce information on the site.

2.0 CELAR ISO9001 PROCESS

CELAR is ISO9001 since 1998.

The technical process , aimed to "assist project manager for their internet services project" , was introduced into our quality system in 2001.

1.1 Process input

It is required to meet the project manager to exchange : explanation on applicable laws and directives, project documentation, project timeline, outcontracting requirements etc …

Internet Service Provider ISP's assessment is based on questionnaire (that can be sent within the procurement process) and on site visit for final selectionned ISP. Data collected with these imputs are used to produce the outputs.

1.2 Process output

Expertise on project documentation is the first job : missing requirements are added, questions related to information security : supplier organization, project management, existing infrastructures or previous projects.

Expertise on system architecture : the solution proposed by the supplier is reviewed to reveal architecture weaknesses or vulnerabilities.

Expertise on ISP « maturity » : with the questionnaire and on site visit, this maturity is evaluated. An action plan is proposed both for ISP and project manager. Indeed, not only the supplier can improve his process, organization or technical solution, but the project manager has some tasks to complete in order to meet the MoD requirements previously listed.

1.3 Process tools

Models of reports are used to minimize the delivery delay. The questionnaire is a short check-list about the following topics :

- security policy : level of formalization and use : steering committee, training, responsibility …
- organization : description of jobs involved and responsible for security
- procedures : description, how are they diffused, known and verified
- physical security : description
- networks : availability, remote access
- backup
- security survey : subjects, who, how
- security configuration : who, how, relevance, coherence, test and validation
- audit : who specifies and uses internal audit logs, warning procedure, external assessment, previous alerts management.

1.4 Process improvement

Written in 2001, this process was updated in 2003 : a new model of reports was added.

3.0 SYSTEM SECURITY ENGINEERING-CAPABILITY MATURITY MODEL

Reader is invited to read [4] for complete explanation on SSE-CMM.

Short citations of SSE-CMM are under Copyright © 1999 Systems Security Engineering Capability Maturity Model (SSE-CMM) Project

Please note that no appraisal compliant with SSE-CMM have been done for the following paragraphs, it’s just an exercice ☺.

We will only study in this paper this model as a “basis for security engineering evaluation organizations to establish organizational capability-based confidences”.
For the purpose of contracting internet services, there are three actors in this process : the project manager, the ISP and the MoD expert.

The three main area of the security engineering process are : engineering, risk and assurance process. The three actors are involved in these 3 area depending on the process area studied.

A capability level from 1 to 5 is determined for each process area :

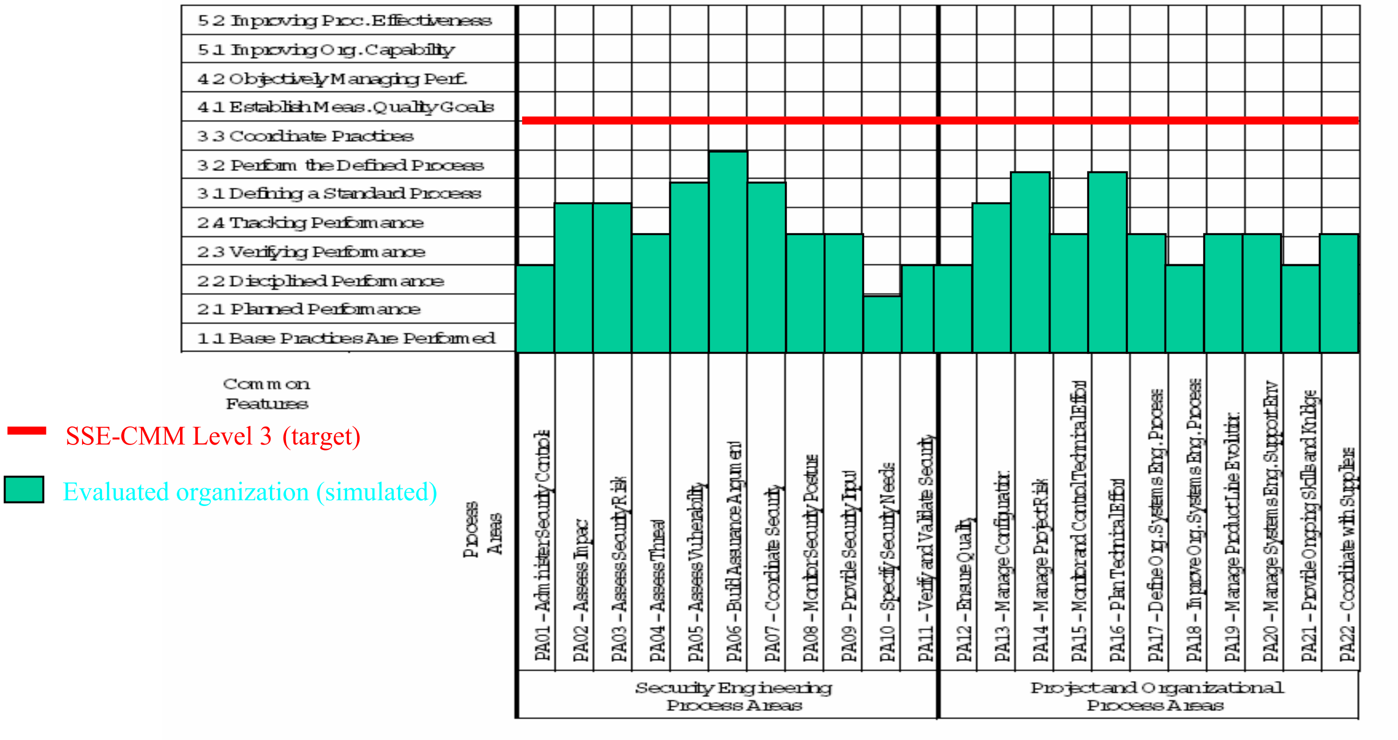

Figure 1: capability level (simulation)

In this simulated case, we see that level 3 is not reached, level 2 neither. If we try to measure the effort to reach level 3 by using the following metrics : 1 point for 1 step, we find 91 points. This metrics is not good enough because effort is not the same along process area and level steps but it’s enough for our study.

Action plan to reach level 3 would be conducted for each of the three actors : let’s say 70 points for the ISP, 15 for project manager and 6 points for MoD expert.

4.0 EXTENSION TO SSE-CMM : ADAPTATIVE CONFIDENCE PROFILE

This model can be improved by 2 ways for our purpose :

- ISP don’t need to reach a full SSE-CMM level to match our needs (full compliance costs time and money)
- the level of assurance depends on the system and the environment (it might be modified by AWR – Alert Warning Response - levels for example)

We propose the use of an « adaptative confidence profile »

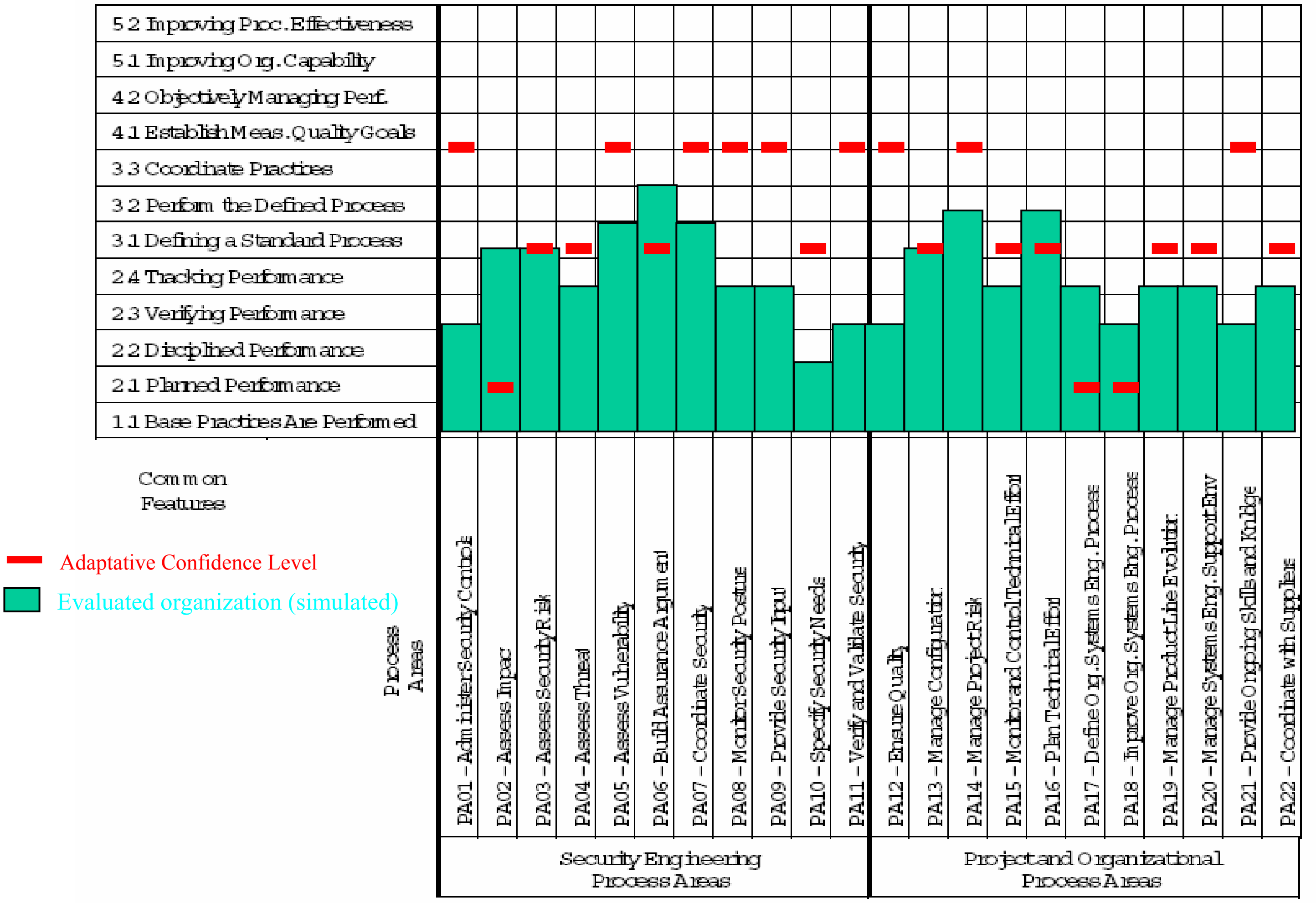

Figure 2: adaptative confidence level (simulation)

In this simulated case, we see that our confidence level is sometimes not reached, sometimes exceeded. If we try to measure the effort to reach our confidence level by using the previous metrics : 1 point for 1 step, we find 42 points. We can also see that it exceeds our needs by 12 points.

Action plan to reach our confidence level would be conducted for each of the three actors : let’s say 21 points for the ISP, 15 for project manager and 6 points for MoD expert.

Let’s comment this, if MoD expert and project manager probably had the same amount of work , the benefit would be first for the ISP who would divide by 2,5 the amount of work, but the major benefit would be for the project cost : the less time we spend, the more money we earn for the same level of confidence. The exceeding levels should be studied to reduce cost too.

The main difficulty is the definition of the confidence profile but another advantage is the ability to match this with AWR levels. For example, to prepare all levels of warnings but only spend money during high level of warning, and reduce cost of ownership during low level of warning.

5.0 RESULTS [1998-2003]

- First period allow to construct and simplify our process
- Second period (until now) dedicated to improve this process
- Divide time and charge of expert by 2.5 between 1998 and 2003.
- ISP improved their security during this period : this is demonstrated by ISP that have been evaluated at least twice

6.0 LESSONS LEARNED

- security label for ISP (ISO12207, IS17799) is not enough : some ISP have such a label but the perimetrer is not always the same required by our projects, another analysis should be done to analyse differences between these bests pratices.
- People and organizations are major risk factors.
- Project manager is the « key » for success
- Adaptative confidence profil is useful for
  - the expert (assessment time)
  - the project manager (adaptative confidence)
  - the evaluated organization (money)

[1] Instruction n°1829/DEF/CAB/CM/3 relative à la charte de nommage Internet du ministère de la défense : http://www.defense.gouv.fr/creasite/txt_instruction1829.htm

[2] Instruction n°1830/DEF/CAB/CM/3 relative à la mise en œuvre de services en lignes ou de sites Internet par les états majors, directions et services du ministère de la défense : http://www.defense.gouv.fr/creasite/txt_instruction1830.htm

[3] Instruction ministérielle n°8192/DEF/CAB/CM3 relative aux modalités d’accès et à l’utilisation d’Internet au sein du ministère. http://www.bo.sga.defense.gouv.fr/visualisation.aspx?JOB=03PP31&PAGE=5182

[4] System Security Engineering-Capability Maturity Model - Model Description Document version 2.0 April 1999 http://www.sse-cmm.org/model/ssecmmv2final.pdf