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 governmental 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.
1. REPORT DATE 01 NOV 2004
2. REPORT TYPE N/A
3. DATES COVERED -

4. TITLE AND SUBTITLE
Contracting out Governmental Web Services (Externalisation de l’hébergement de sites web gouvernementaux)

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
DGA/DCE/CELAR BP7419 35174 Bruz France

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR’S ACRONYM(S)

11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM001845, Adaptive Defence in Unclassified Networks (La defense adaptative pour les reseaux non classifies),. The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:
   a. REPORT unclassified   b. ABSTRACT unclassified   c. THIS PAGE unclassified

17. LIMITATION OF ABSTRACT UU
18. NUMBER OF PAGES 24
19a. NAME OF RESPONSIBLE PERSON

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18
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
Readers are 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 exercise.

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:

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 »

![Diagram](attachment:image.png)

**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 perimeter is not always the same required by our projects, another analysis should be done to analyse differences between these bests practices.
• 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)


[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](http://www.defense.gouv.fr/creasite/txt_instruction1830.htm)


MINISTÈRE DE LA DÉFENSE

ADAPTATIVE DEFENSE IN UNCLASSIFIED NETWORKS

IST-041-RSY-013

Contracting out governmental web services
Agenda

- Contracting Internet Services for MoD
- CELAR ISO9001 process: input, output, tools and process improvement
- System Security Engineering-Capability Maturity Model
- Extension to SSE-CMM: Confidence Profile
- Some results [1998-2003]
- Lessons learned
Contracting Internet Services for MoD

- Usage of Internet Services is defined by MoD directives (IM1829 - IM1830 - IM8192)
- IM1830 advise the project manager to use CELAR expertise for security aspects
- Basic requirements are: domain naming(.gouv.fr), integrity, availability, imputability.
CELAR savoir faire : input

- meetings with project manager
- project documentation
- ISP assessment : based on questionnaire and on site visit for final selectionned ISP.
CELAR savoir faire : output

- Expertise on project documentation
- Expertise on system architecture
- Expertise on ISP « maturity »
- Action plan for ISP and project manager
CELAR savoir faire: tools and process improvement

- CELAR added a processus description for this expertise in 2001 (PT604a), this process was updated in 2003 (PT604b)
- Tools are:
  - a questionnaire
  - models of reports
CELAR ISO9001 savoir faire : questionnaire topics

- 1 - Security policy
- 2 - Organization
- 3 - Procedures
- 4 - Physical security
- 5 - Networks
- 6 - Backup
- 7 - Security survey
- 8 - Security configuration
- 9 - Audit
The Systems Security Engineering Capability Maturity Model (SSE-CMM) describes the essential characteristics of an organization’s security engineering process that must exist to ensure good security engineering.

The SSE-CMM and the appraisal method are intended to be used as a (...) basis for security engineering evaluation organizations to establish organizational capability-based confidences (...)

System Security Engineering-Capability Maturity Model
Model Description Document version 2.0 april 1999
Copyright © 1999 Systems Security Engineering Capability Maturity Model (SSE-CMM) Project
Permission to reproduce this product and to prepare derivative works from this product is granted royalty-free, provided the copyright is included with all reproductions and derivative works.

The Systems Engineering CMM is "Copyright © 1995 by Carnegie Mellon University. This work is a collaborative effort of Hughes Space and Communications, Hughes Telecommunications and Space, Lockheed Martin, Software Engineering Institute, Software Productivity Consortium, and Texas Instruments Incorporated. Permission to reproduce this product and to prepare derivative works from this product is granted royalty-free, provided the copyright is included with all reproductions and derivative works."
Figure 3.1 – The security engineering process has three main areas.

System Security Engineering-Capability Maturity Model
Model Description Document version 2.0 April 1999
Copyright © 1999 Systems Security Engineering Capability Maturity Model (SSE-CMM) Project
Figure 3.2 – The security risk process involves threats, vulnerabilities, and impact.
Figure 3.3 – Security is an integral part of the overall engineering process.
Figure 3.4 – The assurance process builds an argument establishing confidence.
FIGURE 3.6 — Capability levels represent the maturity of security engineering organizations.
SSE-CMM 2.0

5.2 Improving Proc. Effectiveness
5.1 Improving Org. Capability
4.2 Objectively Managing Perf.
4.1 Establish Meas. Quality Goals
3.3 Coordinate Practices
3.2 Perform the Defined Process
3.1 Defining a Standard Process
2.4 Tracking Performance
2.3 Verifying Performance
2.2 Disciplined Performance
2.1 Planned Performance
1.1 Base Practices Are Performed

Common Features

SSE-CMM Level 3 (target)
Evaluatted organization (simulated)
SSE-CMM 2.0 and confidence profile

This model may 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 cost time and money)

- the level of assurance depend on the system and the environment (it might be modified by AWR levels for example)

-> We propose the use of an « adaptative confidence profile »
### SSE-CMM 2.0 and confidence profile

<table>
<thead>
<tr>
<th>Process Areas</th>
<th>Security Engineering Process Areas</th>
<th>Project and Organizational Process Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>EA01 - Define Security Functionality</td>
<td>FA01 - Define Security Functionality</td>
<td>EA01 - Define Security Functionality</td>
</tr>
<tr>
<td>EA02 - Define Security Organization</td>
<td>FA03 - Define Security Organization</td>
<td>EA04 - Define Security Organization</td>
</tr>
<tr>
<td>EA03 - Define Security Policy</td>
<td>FA05 - Define Security Policy</td>
<td>EA06 - Define Security Policy</td>
</tr>
<tr>
<td>EA05 - Define Security Architecture</td>
<td>FA09 - Define Security Architecture</td>
<td>EA10 - Define Security Architecture</td>
</tr>
<tr>
<td>EA06 - Define Security Artefacts</td>
<td>FA11 - Define Security Artefacts</td>
<td>EA12 - Define Security Artefacts</td>
</tr>
<tr>
<td>EA14 - Manage Product Life Cycle</td>
<td>FA21 - Manage Security Needs</td>
<td>EA22 - Coordinate with Suppliers</td>
</tr>
<tr>
<td>EA15 - Manage Systems Engineering</td>
<td>FA22 - Coordinate with Suppliers</td>
<td></td>
</tr>
<tr>
<td>EA16 - Plan Technical Debt</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Common Features
- **A** adaptative confidence profile
- **E** evaluated organization (simulated)
Some 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
- ISP improved their security during this period
Lessons learned

- Security label for ISP (ISO12207, ISO17799) is not enough?
- People and organizations are major risk factor
- 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)