Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'INTÉRIEUR

EXAMEN PROFESSIONNEL D'ACCES AU GRADE D'INGENIEUR PRINCIPAL DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

- SESSION 2018 -

Mardi 13 mars 2018

SUJET N° 2

Etude de cas à partir de deux dossiers techniques de trente pages maximum, soumis au choix du candidat le jour de l'épreuve écrite, permettant de vérifier les capacités d'analyse et de synthèse du candidat ainsi que son aptitude à dégager des solutions appropriées.

(Durée : 4 heures – Coefficient 1)

Le dossier documentaire comporte 26 pages.

IMPORTANT

IL EST RAPPELE AUX CANDIDATS QU'AUCUN SIGNE DISTINCTIF NE DOIT APPARAITRE NI SUR LA COPIE NI SUR LES INTERCALAIRES.
ECRIRE EN NOIR OU EN BLEU - PAS D'AUTRE COULEUR

SUJET

ETUDE DE CAS

Contexte :

L'organisme de gestion interministérielle des concours (OGIC) organise pour l'ensemble des ministères plus de 1 000 concours donnant lieu à la correction d'environ 1 000 000 copies. Ces concours sont organisés dans une cinquantaine de centres d'examen appartenant à l'OGIC.

Les concours sont constitués d'un écrit et d'un oral.

Pour chaque concours, l'OGIC a recours à des concepteurs et à des correcteurs de sujets pour réaliser en moyenne 3 sujets par concours. Le concepteur du sujet peut être aussi correcteur du sujet mais ce n'est pas systématique.

Cette phase d'élaboration des sujets dure en moyenne 3 semaines et nécessite le déplacement des concepteurs de sujets. Les sujets sont soumis à la validation d'un jury constitué d'un président et de 4 membres, non permanents et issus des différents ministères, tout comme les concepteurs et les correcteurs des sujets.

Chaque sujet est constitué en moyenne de 40 pages qui vont faire l'objet d'un tirage papier par les services de l'OGIC au profit des candidats.

Après les épreuves, l'ensemble des copies est collecté par l'OGIC et est remis pour correction aux correcteurs. Cela pose des difficultés logistiques, les correcteurs étant répartis sur l'ensemble du territoire français. Outre ces aspects, il y a des risques de perte de documents ou de vols.

A l'issue des corrections, le jury ainsi que les correcteurs se réunissent afin de définir la liste des personnes admissibles à présenter l'oral.

Dans une démarche de simplification et de sécurisation, l'OGIC lance un projet visant à dématérialiser les phases de préparation des sujets et de correction des copies.

L'application envisagée doit permettre de réaliser les 3 fonctions suivantes en garantissant la confidentialité et l'intégrité des données manipulées :

- les concepteurs déposent les sujets finalisés pour traitement par les équipes de l'OGIC chargées de la mise en forme et de leur édition, après validation par le jury. Il s'agit d'un fichier texte accompagné d'une ou plusieurs pièces jointes de documents.
- l'OGIC numérise les copies des candidats afin de permettre aux correcteurs d'y avoir accès via un site web sécurisé. La partie relative à la gestion des notes sera prise en compte dans un second temps et ne doit pas être traitée dans votre réponse.
- les correcteurs accèdent aux copies à corriger.

L'ensemble des données sera stocké pendant 5 ans.

Demande :

Vous avez été nommé le 13 mars 2018 chef du projet GDC (gestion dématérialisée des concours) par votre sous-directeur. Une réunion de cadrage est organisée entre votre directeur, le directeur de l'OGIC et le responsable de la sécurité des systèmes d'information (RSSI) afin de voir la faisabilité de l'opération et le délai nécessaire pour sa réalisation.

Cette nouvelle application doit être opérationnelle pour le 01/01/2019 au plus tard.

Pour sa réunion, vous devez remettre à votre directeur une fiche décrivant les éléments suivants :

- un schéma simplifié de l'architecture technique, logicielle et fonctionnelle mise en œuvre. Vos choix devront être justifiés (**9 points**) ;
- un planning projet décrivant les différentes phases de votre projet avec les profils techniques nécessaires, une estimation des charges associées et la gestion des risques associée (**8 points**) ;
- une description des mesures mise en œuvre pour garantir la sécurité et le bon fonctionnement de cette application (**3 points**).

Cette fiche doit permettre d'avoir une vision précise sur la faisabilité de ce projet dans le temps imparti.

Pour les schémas, vous pouvez utiliser toutes les représentations que vous souhaitez (UML, merise,…).
Vous serez évalué sur le fond et non le formalisme utilisé.

Dossier documentaire :

Document 1	Les indicateurs de performance Source : http://www.relationclientmag.fr/Thematique/techno-solutions-it-1016/Breves/Les-indicateurs-mesurer-performance	Pages 1 à 3
Document 2	Le catalogue de service de la DSIC	Page 4
Document 3	L'homologation de sécurité Source : http://ssi.minint.fr	Page 5
Document 4	Le cadre de cohérence technique ministériel – extrait	Pages 6 à 9
Document 5	TOP 10 de OWASP Source : https://www.owasp.org	Pages 10 à 15
Document 6	Qualité logicielle Source : https://fr.wikipedia.org/wiki/Qualité_logicielle	Pages 16 à 19
Document 7	Gestion des risques d'un projet Source : https://fr.wikipedia.org	Pages 20 à 25
Document 8	Sécurité : sécuriser les sites web Source : https://www.cnil.fr/fr/securite-securiser-les-sites-web	Page 26

Source : www.relationclientmag.fr - "Les indicateurs pour mesurer sa performance"

Taux de résolution au premier contact, Net Promoter Score, CES, score de satisfaction, analyse du churn... les indicateurs pour mesurer la performance de son service client son nombreux. Leur but? Piloter et améliorer la qualité du service rendu au client mais aussi agir sur la motivation des équipes et créer une dynamique de groupe.

1. Le CSAT: classique mais incontournable

   Le CSAT, pour Customer Satisfaction, soit la satisfaction client, est sans doute l'indicateur le plus utilisé par les entreprises. Répondant à la question "Avez-vous été satisfait ?", il permet de mesurer si le client a apprécié son expérience ou encore un produit ou un service spécifique. La réponse est souvent simple, "oui" ou "non", mais il peut aussi être demandé au client d'attribuer une note ou un nombre d'étoiles. Le smiley -content, neutre ou en colère- est également répandu. Cet indicateur permet de piloter son service de relation client à condition de creuser un peu quels points précis de l'expérience, du produit ou du service ont été appréciés ou non. Il est par ailleurs beaucoup utilisé par les entreprises dans leur communication, affichant sur le Web ou ailleurs leur taux de satisfaction client ou le nombre d'étoiles qui leur a été attribué. C'est un vrai outil de la réputation et de l'e-réputation.
2. Le temps d'attente: toujours important

   Les clients n'aiment pas attendre. Surtout quand ils essayent de joindre un service client pour régler un problème. C'est pourquoi l'indicateur du temps d'attente est toujours incontournable. D'ailleurs, le référentiel NF345 (NF Service- Relation client) exige des entreprises certifiées qu'elles répondent à 80 % des appels en moins de 1 minute et 30 secondes. Preuve que cette notion d'attente est toujours au coeur des préoccupations des entreprises qui souhaitent soigner leur relation client.

3. La résolution au premier appel détrône le délai moyen de traitement

   Il fut un temps où le délai moyen de traitement (DMT) était roi: la course était aux conseillers qui réglaient un problème client en lui accordant le moins de temps possible. C'était sans compter sur le fait que les clients rappelaient par la suite, leur problématique ayant finalement été mal traitée. Ce qui générait des coûts supplémentaires et de l'insatisfaction client. C'est pourquoi un nouvel indicateur est apparu: la résolution au premier appel (First call resolution, FCR). L'objectif n'est plus d'expédier en quelques minutes une question client mais de prendre le temps d'y répondre et de s'assurer que le client n'a pas d'autres questions avant de mettre fin à la conversation. Pour qu'il soit satisfait dès son premier appel et ne rappelle pas.

4. Les entreprises ne jurent plus que par le NPS Pas d'indicateur de mesure de la relation client sans NPS! En quelques années, le Net Promoter Score (indicateur de la recommandation) est devenu l'indicateur incontournable, la véritable coqueluche des directeurs de la relation client. La raison: il permet de se comparer aux autres entreprises, de comparer les différents centres/magasins/filiales entre eux, de comparer ses résultats par rapport aux années précédentes, etc. Il se détermine en posant la question "Quelle est la probabilité que vous recommandiez notre

marque/produit à votre entourage?", à laquelle le consommateur répond en attribuant une note de 1 à 10. Le NPS se calcule ensuite en soustrayant le nombre de détracteurs (notes de 1 à 6) aux promoteurs (9 à 10): le score ainsi obtenu, se situant entre -100 et +100, est considéré comme correct s'il est positif, et comme excellent à partir de +50. Un indicateur intéressant mais auquel les entreprises auraient tort de se limiter. En effet, le NPS est plus lié à l'image que l'on a de la marque ou de ses produits qu'à l'expérience client en tant que telle.

5. Le customer effort score au coeur de l'expérience client

   On ne jure plus que par elle: l'expérience client est devenue le graal absolu. Les entreprises cherchent désormais à faire vivre une véritable expérience à leur client, à les enchanter, titiller leurs émotions... L'objectif: être gravées à jamais dans leur souvenir. À condition que l'expérience soit positive et non négative. C'est pourquoi est apparu le Customer effort score (CES), l'indicateur d'effort client. L'objectif est de s'assurer que l'expérience qu'a vécue le client lui a demandé le moins d'efforts possible. Pour le mesurer, les entreprises demandent à leurs clients d'évaluer, sur une échelle de 1 à 5, les efforts qu'ils ont dû déployer pour voir leur demande satisfaite. Le mieux, afin de véritablement évaluer ce qui était positif et ce qui était négatif, est d'y associer des items: temps, compréhension des questions et des réponses, processus clair ou non, etc. Seul bémol: cet indicateur est un peu trop opérationnel, trop déconnecté de l'aspect émotionnel de l'expérience client. Il faut donc le coupler avec un indicateur comme le NPS.

6. Le taux de digitalisation pour s'assurer de sa multicanalité

   Autre dada des entreprises: la digitalisation. Les entreprises se veulent multicanales, et même omnicanales. Pour s'assurer que les clients utilisent bien les canaux digitaux, il existe différents indicateurs. Le taux de digitalisation, tout d'abord, qui consiste à analyser le nombre de contacts par canal afin de mesurer la proportion de contacts traités par les canaux digitaux. À noter également le taux de transfert de contacts vers le self care afin de s'assurer que les demandes simples sont bien prises en charge par les FAQ dynamiques, agents virtuels, chatbots ou encore communautés d'entraide.

7. Analyser son churn

   Si la relation client doit suivre un indicateur, c'est bien celui-là: le churn ou taux d'attrition. En effet, le rôle premier du service de relation client est de s'assurer que les clients n'iront pas voir ailleurs, mais resteront bien fidèles. S'ils partent, c'est l'échec de ce qui a été mis en oeuvre. À suivre de près mais en le disséquant pour comprendre pourquoi il n'a pas été possible de retenir tel ou tel client.

8. Le taux de réachat pour mesurer la fidélité Parallèlement au churn, il peut être intéressant de regarder également le taux de réabonnement/de réachat. Cela peut permettre de motiver les équipes, voire de les incentiver. Car quand on travaille à augmenter la fidélité, il est primordial de mesurer le taux de clients fidèles!

9. Estimer le nombre de clients ambassadeurs

   Quand on connaît l'importance du bouche à oreille, avoir des clients ambassadeurs

est incontournable. D'où la bonne idée d'en mesurer le nombre dans l'objectif de l'améliorer. Mais il ne faut évidemment pas en rester là et essayer de bien identifier ces clients ambassadeurs, les connaître pour leur envoyer des informations exclusives afin qu'ils les relaient, mais aussi des cadeaux spéciaux.

10. Le taux de transformation monte en puissance

    De plus en plus, les conseillers en relation client sont chargés de réaliser des ventes. Up selling, cross selling... Il s'agit de mesurer leur efficacité dans ce domaine également. Le taux de transformation devient donc un indicateur à suivre pour toutes les directions de la relation client.

Catalogue de services

Environnement de travail & mobilité

Acquérir, modifier son environnement informatique de travail. Pouvoir accéder à ses SI métier et à des applications disponibles en ligne de manière simple et sécurisée.

- Poste de travail informatique
- Nomadisme
- Téléphonie
- ...

Expertise & ingénierie

Faire réaliser un projet informatique. Disposer d'une assistance et d'une analyse techniques (évolutions ou dysfonctionnements) pour les SI métier. Disposer de conseils en architecture. Bénéficier des supports et de l'expertise juridiques.

- Réalisation d'une application métier
- Réalisation d'une infrastructure technique (téléphonie, vidéo, réseau, ...)
- Assistance à maîtrise d'ouvrage (application, infrastructure)
- Métrologie
- Assistance et expertise juridique pour la passation d'un marché

Sécurité & sûreté

Mettre à disposition les infrastructures SIC sécurisées selon les exigences spécifiques. Délivrer des services ou des prestations de sécurité spécifiques.

- Antivirus
- Certificats numériques
- Signature électronique de documents
- Service d'horodatage
- Appui à la mise en œuvre de la DISSIP
- Appui à l'homologation d'un SI
- ...

Outils collaboratifs

Disposer d'outils de communication, d'outils de travail, d'outils d'accès à la connaissance et d'outils de suivi.

- Messagerie
- Agenda
- Gestion du courrier
- Gestion de la documentation
- Partage de fichiers volumineux
- Visioconférence, salles de réunion
- ...

Hébergement, exploitation & supervision

Faire héberger ses applications ou portails métier. Négocier le niveau de service d'infogérance.

- Hébergement des applications métier
- Contrat de services
- Exploitation d'un système d'information
- Supervision d'un système d'information
- ...

Assistance utilisateurs & soutien de proximité

Faire bénéficier, les utilisateurs d'une application ou les usagers d'un service, du support mis en place par la DSIC.

- Chaîne de soutien utilisateur
- d'une application
- Aide à l'utilisation des offres de services
- de la DSIC
- Soutien de proximité (petits câblages,...)
- ...

Source : ssi.minint.fr

L'homologation de sécurité

L'objectif de la démarche d'homologation est de permettre à la maîtrise d'ouvrage d'un SI de s'assurer que le service offert est conforme à ses attentes.

Au même titre que la Vérification d'aptitude au bon fonctionnement (VABF) est un pré-requis à la mise en production de manière à s'assurer que le SI couvre les besoins fonctionnels, l'homologation atteste de la couverture du besoin de sécurité.

L'homologation de sécurité d'un SI est l'attestation que les besoins de sécurité ont été identifiés et qu'ils sont couverts par des mesures de sécurité. Qu'ainsi les risques résiduels sont maîtrisés et acceptés et que le SI est par conséquent apte à être mis en production.

Dans le cas des SI soumis au Référentiel général de sécurité (RGS), l'exigence de l'homologation est réglementaire. La négliger introduit un risque de contentieux.

En quelques mots

Analyse de risques

Cette phase, en début de projet permet d'évaluer les risques qui pèsent sur un système d'information et de déterminer les objectifs de sécurité qui permettront de les rendre acceptables.

- Combien de temps peut-on se passer du service ?
- Tolère-t-on que des données soient altérées ?
- La divulgation des informations porte-elle préjudice à l'administration ?
- Est-il nécessaire de tracer les actions effectuées sur le système ?

Ce sont des problématiques métier qui doivent être spécifiées à la MOE pour être prises en compte.

Conception et réalisation

Pendant ces phases, la maîtrise d'œuvre élabore le SI qui satisfera les besoins exprimés par la MOA. La MOE détermine puis met en œuvre les éléments les mesures techniques pour atteindre les objectifs identifiés.

Homologation

Les mesures techniques et organisationnelles mises en place permettent de réduire les risques. Il s'agit de vérifier que ceux qui sont suffisamment faibles, en termes d'impact et de vraisemblance, pour pouvoir exploiter sereinement le SI. L'autorité d'homologation peut alors prononcer la décision d'homologation

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'INTÉRIEUR

Secrétariat général
MISSION MINISTÉRIELLE
DE GOUVERNANCE
DES SYSTÈMES D'INFORMATION ET
DE COMMUNICATION

Cadre de Cohérence Technique Ministériel

Présentation générale

Objet

Ce document présente le Cadre de Cohérence Technique (**CCT**) du Ministère de l'Intérieur.

Le CCT a pour but de fixer le cadre technique pour la conception, la réalisation, l'hébergement et l'exploitation de tout système d'information mis en œuvre au Ministère de l'Intérieur.

1. Avertissement

Le cadre de cohérence technique (CCT) du Ministère de l'Intérieur référence par défaut les recommandations des référentiels généraux : référentiel général d'interopérabilité (**RGI**), référentiel général d'accessibilité (**RGAA**), référentiel général de sécurité (**RGS**), référentiel général de gestion des archives (**R2GA**) publiés par le secrétariat général pour la modernisation de l'action publique (SGMAP) [D1], **la charte internet de l'État** [D2] et le socle interministériel des logiciels libres (SILL) [D3]. A l'exception du SILL qui est un cas particulier, il ne reprend les différentes règles ou recommandations de ces documents de référence qu'en cas de **restriction d'usage ou de complément spécifiques au contexte du ministère**.

En ce qui concerne le SILL, c'est le référentiel de produits du CCT qui a la priorité : en effet tous les produits référencés au SILL ne sont pas nécessairement inscrits au CCT. En conséquence, concernant le référentiel de produits du CCT, les règles suivantes s'appliquent :

- le référencement SILL est explicitement signalé par le commentaire « Inscrit au SILL ».
- quand la version préconisée est celle du SILL, cela est également indiqué explicitement par la mention « Version SILL ».
- l'usage d'un produit du SILL non inscrit au CCT doit faire l'objet d'un signalement auprès du référent CCT de l'acteur SIC dont vous relevez.

En conséquence, les référentiels du SGMAP, la charte internet de l'État et le présent CCT devront être référencés dans les cahiers des charges (CCTP) en y intégrant la formulation suivante :

Le ministère de l'intérieur a spécifié et maintient à jour un ensemble de règles et recommandations concernant les composants techniques (logiciels en particulier) devant être utilisés dans le cadre des projets et systèmes mis en œuvre au sein de son système d'information. Ces règles et recommandations sont rassemblées au sein du cadre de cohérence technique (CCT) joint en annexe au présent document.

Le soumissionnaire, dans sa proposition, détaille de manière claire et synthétique les choix qu'il effectue, en précisant, pour chaque composant logiciel :

1. s'il s'agit d'un composant libre présent au CCT, les principaux points techniques justifiant ce choix,

2. s'il s'agit d'un composant non libre présent au CCT, les raisons qui poussent le soumissionnaire à le préférer à un composant libre existant. Ces motifs doivent faire apparaître comme incontestables les gains pour l'administration, soit en terme financiers, soit dans une perspective de long terme, soit en termes de délais de réalisation, soit en termes de risques critiques pour le projet,

3. s'il s'agit d'un composant libre non inscrit au CCT ou au SILL, les raisons qui poussent le soumissionnaire à le préférer au(x) composant(s) libre(s) référencé(s) par le CCT ou le SILL. Dans ce cas, la comparaison portera notamment avec le composant libre correspondant présent au CCT ou au SILL, dans le cas où le CCT ou le SILL référencent un composant de ce type,

4. s'il s'agit d'un composant non libre et non inscrit au CCT, les raisons qui poussent le soumissionnaire à le préférer au(x) composant(s) référencé(s) par le CCT, suivant une présentation identique à celle du point 2 ci-dessus mais étendue à la comparaison avec le ou les éventuel(s) composant(s) non libre(s) référencés par le CCT.

Si pour un contexte donné, le chef de projet juge qu'une règle ou recommandation est incontournable, il doit alors la transférer dans son CCTP et préciser son caractère obligatoire. Cette exigence sera alors reprise dans le Cadre de Conformité et évaluée en tant qu'élément de conformité de l'offre, c'est à dire qu'une proposition ne respectant pas cette exigence sera automatiquement rejetée.

Toute difficulté rencontrée lors de la mise en œuvre du cadre de cohérence technique devra être signalée à la Mission de Gouvernance Ministérielle des SIC.

2. Objectifs

Conformément à ce qui est défini dans le schéma directeur des SIC, la gouvernance ministérielle doit disposer de référentiels partagés, notamment d'un cadre de cohérence technique (CCT).

Cet outil de normalisation commun, au service d'une stratégie, est applicable à l'ensemble des acteurs du ministère et doit répondre aux enjeux actuels, à savoir permettre à chacun de disposer d'un système d'information robuste, efficient, sécurisé, évolutif, et à moindre coût.

Le CCT, au service de la stratégie ministérielle, doit permettre de :

- fournir aux utilisateurs finaux un service de qualité ;
- simplifier les architectures existantes ;
- disposer d'un bon niveau de sécurité.
- valoriser les compétences internes ;
- permettre aux chefs de projet de garantir la cohérence du système d'information à l'aide de documents de référence ;
- maîtriser les coûts.

Pour y parvenir, il est nécessaire de :

- respecter les normes et standards (utilisation de standards ouverts) pour assurer une bonne interopérabilité entre systèmes ;
- définir un socle technique commun par domaine ;
- diminuer le nombre de technologies utilisées (recherche d'homogénéité);
- disposer d'un système d'information évolutif et modulaire ;
- garantir la maintenabilité et l'évolutivité des systèmes ;
- garantir la ré-utilisabilité des composants du SI (architecture, infrastructure, sécurité, services, développement) ;
- garantir la réversibilité des projets (prise de connaissance et rétro-ingénierie) ;
- fédérer les acteurs SIC autour de la stratégie ministérielle.

NB : Concernant la maîtrise des coûts, le CCT a pour objectif de proposer systématiquement une alternative open source aux logiciels propriétaires.

3. Organisation du corpus CCT

Le CCT est organisé en 2 grandes sections :

- les documents généraux, coeur du CCT, avec une présentation générale, les référentiels de règles et de produits, la liste des autres référentiels
- les documents annexes - Certains d'entre eux s'appliquent au périmètre ministériel, les autres ont un périmètre restreint à un seul acteur SIC (DSIC, ST(SI)², PP ...)

L'ensemble du corpus est publié sur l'intranet de la MGMSIC.

4. Cadre d'utilisation

Lors de la conception des projets, la conformité au cadre de cohérence technique doit être vérifiée. L'objectif est de vérifier la bonne intégration au SI ministériel.

Le CCT (dans sa partie “Référentiel de règles”) définit deux niveaux de préconisation :

- La **règle**: il s'agit d'une préconisation à respecter a priori, sauf à ce que le candidat démontre qu'elle n'est pas applicable au contexte du projet ou que ne pas la respecter procure un avantage significatif pour l'administration ;
- La **recommandation**: elle a pour but de guider les choix et marque une préférence de l'administration. Il va de soi qu’en tant que recommandation, son application peut être plus librement modulée.

La conformité des projets au cadre de cohérence technique doit être vérifiée :

- au lancement ;
- à la conception ;
- à la mise en production.

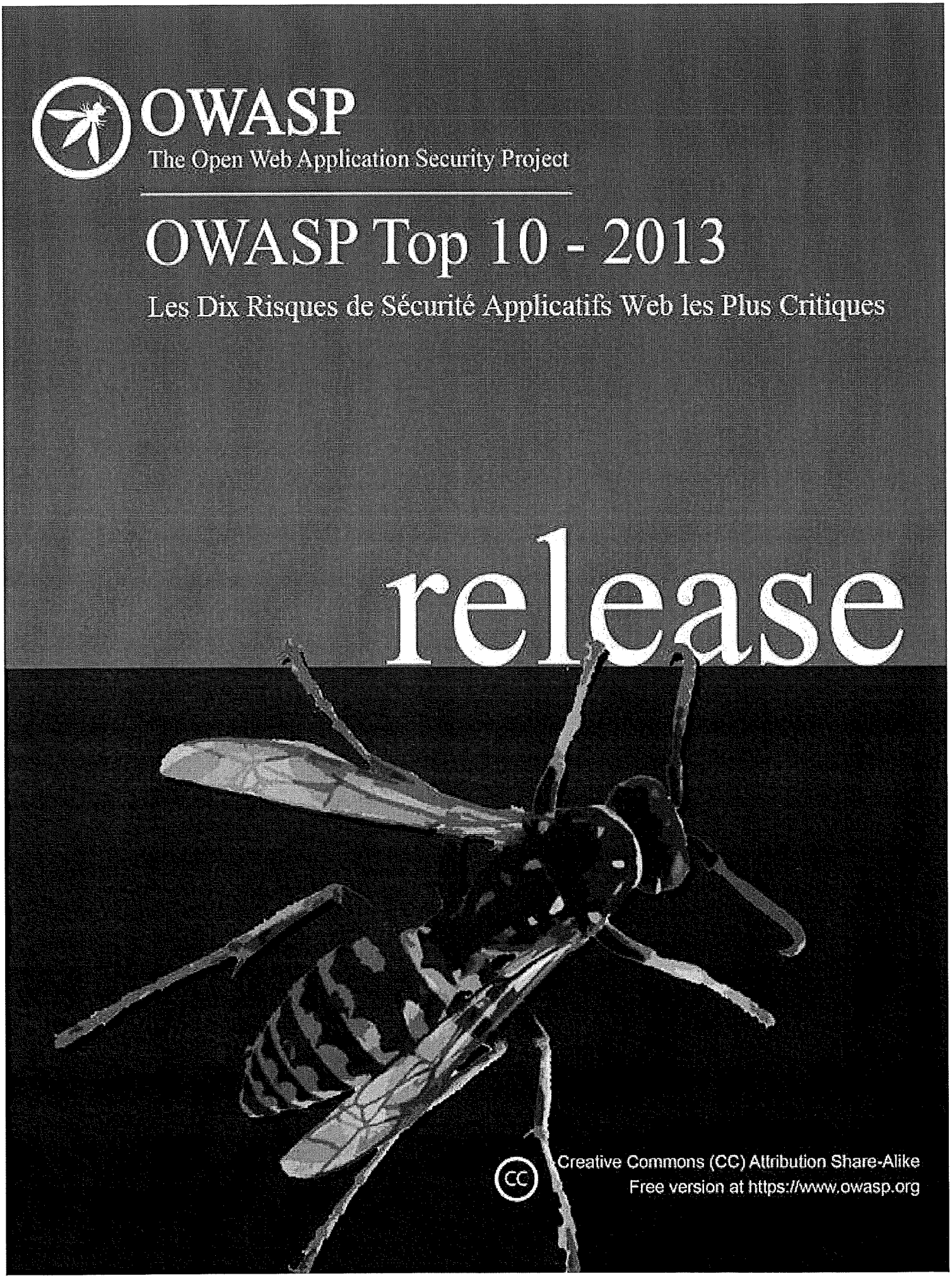
Dans le cadre de projet sous-traités, les vérifications supplémentaires suivantes seront réalisées :

- au lancement de l'appel d'offre ;
- au dépouillement (grille de conformité au CCT et notation).

5. Évolution du Cadre de Cohérence Technique

Le CCT est amené à évoluer continuellement. Ses sources d'évolution sont aussi bien internes (constatation d'obsolescence d'un produit ou d'une solution, apport direct d'un constructeur, stratégie technique …) qu'externes (proposition novatrice dans une réponse à un cahier des charges, par exemple).

Le CCT est mis à jour semestriellement (*début et milieu d'année*). Des addenda (mises à jour mineures) peuvent être publiées tous les deux mois environ.


OWASP
The Open Web Application Security Project
OWASP Top 10 - 2013
Les Dix Risques de Sécurité Applicatifs Web les Plus Critiques
release
Creative Commons (CC) Attribution Share-Alike
Free version at https://www.owasp.org

O A propos de l'OWASP

Préface

Les logiciels non sécurisés sapent nos infrastructures critiques telles la finance, la santé, la défense, l'énergie et autres. Notre infrastructure numérique devenant de plus en plus complexe et interconnectée, la difficulté de parvenir à une sécurité des applications augmente de façon exponentielle. Nous ne pouvons plus nous permettre de tolérer les problèmes les plus simples comme ceux présentés dans ce Top 10 OWASP.

Le but de ce projet est de sensibiliser à la sécurité des applications en identifiant certain des risques les plus critiques rencontrés par les entreprise. Ce top 10 est référencé par de nombreuses normes, livres, outils et organisations telles MITRE, PCI DSS, DISA, FTC et bien d'autres. Cette version du Top 10 OWASP marque la onzième année de ce projet de sensibilisation à l'importance des risques de sécurité des applications. La première publication du Top 10 date de 2003, avec des mises à jour mineures en 2004 et 2007. La version 2010 a été réorganisée afin de prioriser par risque, et non juste par prédominance. Cette édition 2013 suit la même approche.

Nous vous encourageons à utiliser ce Top 10 pour que votre entreprise entame une démarche pour la sécurité des applications. Les développeurs peuvent apprendre des erreurs des autres. Les dirigeants devraient commencer à réfléchir sur la façon de gérer le risque que les logiciels créent dans leurs entreprises.

Sur le long terme, nous vous encourageons à créer un programme de sécurité des applications compatible avec la culture et la technologie d'entreprise. Ces programmes sont de toutes formes et tailles, et vous devez éviter de tenter de tout faire en un modèle de processus. Au lieu de cela, tirez parti des points forts de votre entreprise et mesurez ce qui fonctionne pour vous.

Nous espérons que ce Top 10 est utile à vos efforts. N'hésitez pas à contacter l'OWASP pour vos questions, commentaires et idées, soit publiquement à owasp-topten@lists.owasp.org ou à dave.wichers@owasp.org en privé.

L'OWASP

Open Web Application Security Project (OWASP) est une communauté publique permettant à des organismes de développer, acheter et maintenir des applications fiables. A l'OWASP, vous trouverez en accès libre et gratuit...

- Des normes et des outils de sécurité des applications
- Des livres complets sur les tests de sécurité des applications, le développement de code sécurisé et l'audit de code
- Des normes de contrôles de sécurité et des librairies
- Des Chapitres locaux dans le monde entier
- De la recherche de pointe
- Des conférences à travers le monde
- Des listes de diffusion
- Et bien plus... le tout sur www.owasp.org/
- Y compris : www.owasp.org/index.php/Top_10

L'accès à tous les outils, documents et forums de l'OWASP est gratuit et ouvert à toute personne intéressée par l'amélioration de la sécurité des applications. Nous préconisons une approche sécurité des applications en tant que problème de personnes, de processus et de technologie, parce que les approches les plus efficaces pour la sécurité des applications nécessitent des améliorations dans tous ces domaines.

L'OWASP est une organisation d'un nouveau genre. Notre liberté vis-à-vis des pressions commerciales nous permet de fournir une information impartiale, pratique et rentable de la sécurité applicative. L'OWASP n'est liée à aucune entreprise technologique, bien que nous soutenions l'utilisation éclairée de technologies de sécurité commerciale. Semblable à de nombreux projets logiciels open-source, l'OWASP produit de nombreux types de supports dans un esprit collaboratif et ouvert.

La Fondation OWASP est l'entité à but non-lucratif qui assure le succès à long terme du projet. Presque tous ceux associés à OWASP sont volontaires, y compris le Board, les Comités globaux, Chapter Leaders, Chefs de Projets et les Membres. Nous soutenons la recherche de sécurité innovante avec des subventions et des infrastructures.

Rejoignez nous !

Copyright et Licence

1 Introduction

Bienvenue

Bienvenue dans cette édition 2013 du Top 10 de l'OWASP! Cette nouvelle version introduit deux catégories étendues par rapport à la version 2010 afin d'inclure d'importantes vulnérabilités. Elle propose également une réorganisation des risques, basée sur leur prévalence. Enfin, une nouvelle catégorie de risque voit le jour: la sécurité des composants tiers. Ces risques, référencés sous « A6 – Mauvaise configuration sécurité » dans la version 2010, ont désormais une catégorie dédiée.

Le Top 10 2013 de l'OWASP est basé sur 8 jeux de données de 7 entreprises spécialisées dans la sécurité des applications, dont 4 sociétés de conseil et 3 fournisseurs d'outils ou de services SaaS (1 statique, 1 dynamique et 1 statique et dynamique). Ces données couvrent plus 500 000 vulnérabilités à travers des centaines d'organisations et des milliers d'applications. Les 10 catégories de risques couvertes par le Top 10 sont sélectionnées et hiérarchisées en fonction de leur fréquence, de leur exploitabilité, de leur détectabilité et de leurs impacts potentiels.

L'objectif principal du Top 10 de l'OWASP est de sensibiliser les développeurs, concepteurs, architectes, décideurs, et les entreprises aux conséquences des faiblesses les plus importantes inhérentes à la sécurité des applications web. Le Top 10 fournit des techniques de base pour se protéger contre ces domaines problématiques à haut risque – et fournit des conseils sur la direction à suivre.

Avertissements

Ne vous arrêtez pas à 10! Il y a des centaines de problèmes qui pourraient influer sur la sécurité globale d'une application web comme indiqué dans le Guide du développeur de l'OWASP et la série des OWASP Cheat Sheets. Ce se sont des lectures essentielles pour quiconque développe des applications web. Des conseils sur la manière de trouver des vulnérabilités dans les applications web sont fournis dans le Guide de Test et le Guide d'audit de Code.

Changement constant. Ce Top 10 évoluera dans le temps. Même sans modifier une seule ligne de code de votre application, cette dernière peut déjà être vulnérable à une attaque à laquelle personne n'a pensé auparavant. Veuillez prendre connaissance des conseils à la fin de ce document dans les sections relatives aux développeurs, vérificateurs et entreprises pour plus d'information.

Pensez positif! Quand vous serez prêt à arrêter de chasser les vulnérabilités et à vous concentrer sur l'établissement de contrôles solides de sécurité des applications, l'OWASP a publié le Standard de Vérification de Sécurité Applicative (ASVS) comme guide pour les entreprises et les auditeurs d'applications sur ce qu'il faut vérifier.

Utilisez les outils sagement! Les failles de sécurité peuvent être complexes et enfouies dans le code source. Dans la plupart des cas, l'approche la plus rentable pour trouver et éliminer ces faiblesses reste l'humain doté de bons outils.

Allez plus loin! Faites de la sécurité une partie intégrante de la culture de votre entreprise. Pour en savoir plus, consultez Open Software Assurance Maturity Model (SAMM) et Rugged Handbook.

Remerciements

Nos remerciements à Aspect Security pour avoir initié, piloté et mis à jour le Top 10 de l'OWASP depuis sa création en 2003, et à ses principaux auteurs: Jeff Williams et Dave Wichers.

ASPECT SECURITY
Application Security Experts

Nous voudrions remercier les entreprises qui ont contribué à supporter la mise à jour 2013 en fournissant leur données sur la fréquence des vulnérabilités:

- Aspect Security
- HP (résultats issus des produits Fortify et WebInspect)
- Minded Security - Statistiques
- Softtek - Statistiques
- TrustWave, SpiderLabs – Statistiques (voir page 50)
- Veracode – Statistiques
- WhiteHat Security Inc. – Statistiques

Nous tenons également à remercier toutes les personnes ayant contribué aux versions précédentes du Top 10, sans lesquelles , il ne serait pas ce qu'il est aujourd'hui. Sans oublier ceux ayant contribué par leur contenu significatif ou la relecture de cette version 2013:

- Adam Baso (Wikimedia Foundation)
- Mike Boberski (Booz Allen Hamilton)
- Torsten Gigler
- Neil Smithline (MorphoTrust USA) – pour la version wiki et ses commentaires.

RN Notes de version

Ce qui a changé de 2010 à 2013

Le paysage des menaces des applications de sécurité évolue constamment. Les facteurs clé de cette évolution sont les progrès réalisés par les attaquants, l'émergence de nouvelles technologies avec de nouvelles faiblesses, ainsi que des défenses plus intégrées, et le déploiement de systèmes de plus en plus complexes. Pour suivre le rythme, nous mettons périodiquement à jour le Top 10 de l'OWASP. Dans cette version 2013, nous avons apporté les modifications suivantes:

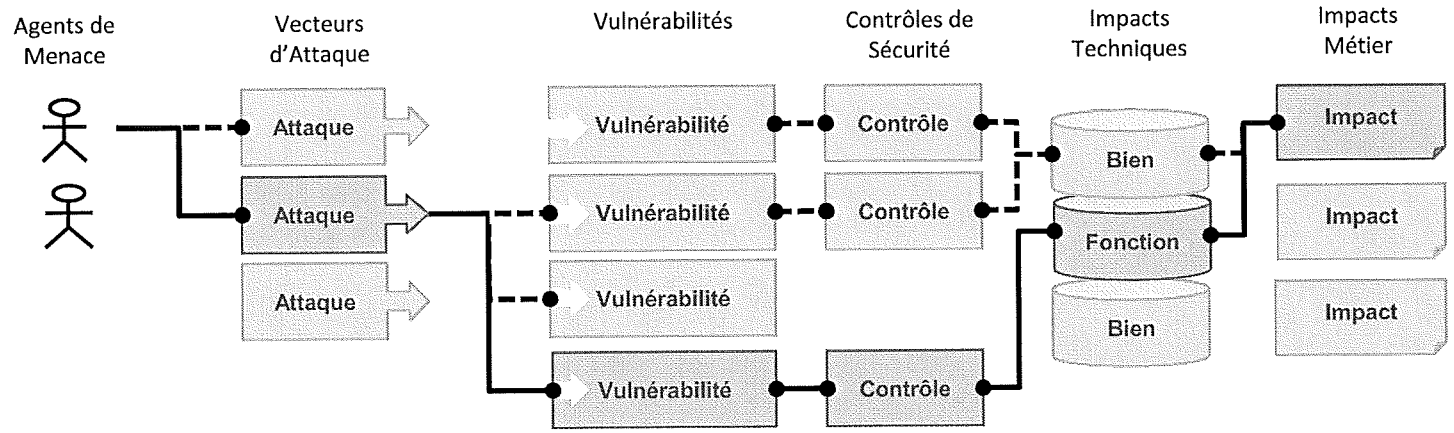
1) La violation de gestion d'authentification et de session est plus répandue selon notre échantillon. Nous pensons que c'est probablement du au fait que ce domaine est plus étudié, et non du fait de problèmes plus répandus. Les risques A2 et A3 changent donc de place.
2) La falsification de requête intersites (CSRF), à prédominance moins répandue dans notre référentiel, rétrograde de 2010-A5 à 2013-A8. Nous pensons que les entreprises et les développeurs ont significativement réduit le nombre de vulnérabilités CSRF dans leurs applications du fait de sa présence dans le Top 10 OWASP depuis 6 ans.
3) Nous avons élargi le Manque de restriction d'accès à une URL du Top 10 d'OWASP 2010 afin d'être plus complet:
   + 2010-A8: Manque de restriction d'accès à une URL est désormais, 2013-A7: Manque de contrôle d'accès au niveau fonctionnel – pour couvrir tous les contrôles d'accès au niveau fonctionnel. Il existe de nombreuses manières de définir quelle fonctionnalité doit être accédée, pas seulement l'URL.
4) Nous avons fusionné et élargi 2010-A7 et 2010-A9 pour CREER: 2013-A6: Exposition de données sensibles.
   – Cette nouvelle catégorie a été créée en fusionnant 2010-A7 – Stockage cryptographique non sécurisé & 2010-A9 – Protection insuffisante de la couche de transport, en y ajoutant le risque de données sensibles au niveau du navigateur. Cette nouvelle catégorie couvre la protection des données sensibles (autre que le contrôle d'accès déjà couvert par 2013-A4 et 2013-A7) à partir du moment où les données sensibles sont fournies par l'utilisateur, transmises et stockées dans l'application, et renvoyées ensuite au navigateur.
5) Nous avons ajouté: 2013-A9: Utilisation de composants avec des vulnérabilités connues:
   + Ce problème a été mentionné comme faisant partie de 2010-A6 – Mauvaise configuration de sécurité, mais possède maintenant une catégorie à part entière du fait de la croissance rapide du développement à base de composants qui a significativement augmenté le risque d'utilisation de composants connus comme vulnérables

OWASP Top 10 – 2010 (Précédent)	OWASP Top 10 – 2013 (Nouveau)
A1 – Injection	A1 – Injection
A3 – Violation de Gestion d'authentification et de Session	A2 – Violation de Gestion d'authentification et de Session
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Références directes non sécurisées à un objet	A4 – Références directes non sécurisées à un objet
A6 – Mauvaise configuration sécurité	A5 – Mauvaise configuration sécurité
A7 –Stockage cryptographique non sécurisé – Fusionné avec A9 →	A6 – Exposition de données sensibles
A8 – Manque de restriction d'accès à une URL – Elargie dans →	A7 – Manque de contrôle d'accès au niveau fonctionnel
A5 – Falsification de requête intersites (CSRF)	A8 – Falsification de requête intersites (CSRF)
<inclus dans A6: Mauvaise configuration sécurité>	A9 – Utilisation de composants avec des vulnérabilités connues
A10 – Redirection et Renvois non validés	A10 – Redirection et Renvois non validés

Risque Risques de sécurité applicatifs

Quels sont les Risques de Sécurité des Applications?

Les attaquants peuvent potentiellement utiliser différents chemins à travers votre application pour porter atteinte à votre métier ou à votre entreprise. Chacun de ces chemins représente un risque qui peut, ou pas, être suffisamment grave pour mériter votre attention.



Parfois, ces chemins sont faciles à trouver et à exploiter, et parfois ils sont extrêmement difficiles. De même, le préjudice causé peut n'avoir aucune conséquence, ou faire cesser votre activité. Pour déterminer le risque pour votre entreprise, vous pouvez évaluer la probabilité relative à chaque agent de menace, vecteur d'attaque, et vulnérabilité et les combiner avec une estimation d'impact technique et financier pour votre entreprise. Ensembles, ces facteurs déterminent le risque global.

Quel est Mon Risque?

Le Top 10 OWASP se concentre sur l'identification des risques les plus graves pour un large éventail d'entreprises. Pour chacun de ces risques, nous fournissons des informations générales sur la probabilité et l'impact technique en utilisant le schéma d'évaluation des risques suivant, qui est basé sur la Méthodologie d'évaluation des risques OWASP.

Agent de menace	Vecteurs d'attaque	Prévalence de la vulnérabilité	Détection de la vulnérabilité	Impact Technique	Impact Métier
Spécifique à l'Application	Facile	Très répandue	Facile	Sévère	Spécifiques à l'Application ou au Métier
	Moyen	Commune	Moyen	Modéré	
	Difficile	Rare	Difficile	Mineur	

Vous seul connaissez les caractéristiques de votre environnement et de votre métier. Pour une application donnée, il n'y a peut-être pas d'agent de menace pouvant réaliser un type d'attaque, ou il peut n'y avoir aucun impact technique. C'est pourquoi vous devez évaluer chaque risque pour vous-même, en vous concentrant sur les agents de menace, contrôles de sécurité et impacts métiers relatifs à votre votre entreprise. Nous classons les agents de menace comme spécifiques aux applications, et les impacts métiers comme spécifiques aux applications ou au métier pour indiquer qu'ils sont clairement dépendants des détails de l'application dans votre entreprise.

Le nom des risques dans le Top 10 découle du type d'attaque, du type de faiblesse, ou du type d'impact qu'il peut causer. Nous choisissons des noms qui reflètent les risque de manière précise, et, quand cela est possible, nous nous alignons sur la terminologie la plus répandue pour assurer la meilleure sensibilisation.

Références

OWASP

- Méthodologie d'évaluation des risques OWASP
- Article sur la modélisation Menace / Risque

Externes

- Analyse de s risques de l'information FAIR
- Modélisation des menaces Microsoft (STRIDE et DREAD)

T10 OWASP Top 10 2013 Risques Sécurité des Applications

A1 – Injection	•Une faille d'injection, telle l'injection SQL, OS et LDAP, se produit quand une donnée non fiable est envoyée à un interpréteur en tant qu'élément d'une commande ou d'une requête. Les données hostiles de l'attaquant peuvent duper l'interpréteur afin de l'amener à exécuter des commandes fortuites ou accéder à des données non autorisées.
A2 – Violation de Gestion d'Authentification et de Session	•Les fonctions applicatives relatives à l'authentification et la gestion de session ne sont souvent pas mises en œuvre correctement, permettant aux attaquants de compromettre les mots de passe, clés, jetons de session, ou d'exploiter d'autres failles d'implémentation pour s'approprier les identités d'autres utilisateurs.
A3 – Cross-Site Scripting (XSS)	•Les failles XSS se produisent chaque fois qu'une application accepte des données non fiables et les envoie à un browser web sans validation appropriée. XSS permet à des attaquants d'exécuter du script dans le navigateur de la victime afin de détourner des sessions utilisateur, défigurer des sites web, ou rediriger l'utilisateur vers des sites malveillants.
A4 – Références directes non sécurisées à un objet	•Une référence directe à un objet se produit quand un développeur expose une référence à un objet d'exécution interne, tel un fichier, un dossier, un enregistrement de base de données ou une clé de base de données. Sans un contrôle d'accès ou autre protection, les attaquants peuvent manipuler ces références pour accéder à des données non autorisées.
A5 – Mauvaise configuration Sécurité	•Une bonne sécurité nécessite de disposer d'une configuration sécurisée définie et déployée pour l'application, contextes, serveur d'application, serveur web, serveur de base de données et la plate-forme. Tous ces paramètres doivent être définis, mis en œuvre et maintenus, car beaucoup ne sont pas livrés sécurisés par défaut. Cela implique de tenir tous les logiciels à jour.
A6 – Exposition de données sensibles	•Beaucoup d'applications web ne protègent pas correctement les données sensibles telles que les cartes de crédit, identifiants d'impôt et informations d'authentification. Les pirates peuvent voler ou modifier ces données faiblement protégées pour effectuer un vol d'identité, de la fraude à la carte de crédit ou autres crimes. Les données sensibles méritent une protection supplémentaire tel un chiffrement statique ou en transit, ainsi que des précautions particulières lors de l'échange avec le navigateur.
A7 – Manque de contrôle d'accès au niveau fonctionnel	•Pratiquement toutes les applications web vérifient les droits d'accès au niveau fonctionnel avant de rendre cette fonctionnalité visible dans l'interface utilisateur. Cependant, les applications doivent effectuer les mêmes vérifications de contrôle d'accès sur le serveur lors de l'accès à chaque fonction. Si les demandes ne sont pas vérifiées, les attaquants seront en mesure de forger des demandes afin d'accéder à une fonctionnalité non autorisée.
A8 - Falsification de requête intersite (CSRF)	•Une attaque CSRF (Cross Site Request Forgery) force le navigateur d'une victime authentifiée à envoyer une requête HTTP forgée, comprenant le cookie de session de la victime ainsi que toute autre information automatiquement inclue, à une application web vulnérable. Ceci permet à l'attaquant de forcer le navigateur de la victime à générer des requêtes dont l'application vulnérable pense qu'elles émanent légitimement de la victime.
A9 - Utilisation de composants avec des vulnérabilités connues	•Les composants vulnérables, tels que bibliothèques, contextes et autres modules logiciels fonctionnent presque toujours avec des privilèges maximum. Ainsi, si exploités, ils peuvent causer des pertes de données sérieuses ou une prise de contrôle du serveur. Les applications utilisant ces composants vulnérables peuvent compromettre leurs défenses et permettre une série d'attaques et d'impacts potentiels.
A10 – Redirections et renvois non validés	•Les applications web réorientent et redirigent fréquemment les utilisateurs vers d'autres pages et sites internet, et utilisent des données non fiables pour déterminer les pages de destination. Sans validation appropriée, les attaquants peuvent réorienter les victimes vers des sites de phishing ou de malware, ou utiliser les renvois pour accéder à des pages non autorisées.

Source : wikipedia.org

Qualité logicielle

Un article de Wikipédia, l'encyclopédie libre.

En informatique et en particulier en génie logiciel, la **qualité logicielle** est une appréciation globale d'un logiciel, basée sur de nombreux indicateurs[1].

La complétude des fonctionnalités, la correction et précision des résultats, la fiabilité, la tolérance de pannes, la facilité et la flexibilité de son utilisation, la simplicité, l'extensibilité, la compatibilité et la portabilité, la facilité de correction et de transformation, la performance, la cohérence et l'intégrité des informations qu'il contient sont tous des facteurs de qualité[2].

Contrairement à un matériel, un logiciel est un produit qui n'a pas une fiabilité prédictible, de plus il ne s'use pas dans le temps. Donc une anomalie survient ou ne survient pas dans l'exécution du logiciel, l'anomalie est présente de manière latente et peut ne jamais survenir. La qualité d'un logiciel dépend entièrement de sa construction et des processus utilisés pour son développement, c'est par conséquent un sujet central en génie logiciel. Une appréciation globale de la qualité tient autant compte des facteurs *extérieurs*, directement observables par l'utilisateur, que des facteurs *intérieurs*, observables par les ingénieurs lors des revues de code ou des travaux de maintenance.

Les problèmes de qualité des logiciels, connus depuis les années 1960, sont par ailleurs à l'origine du génie logiciel, la science de la création de logiciels, y compris toutes les difficultés qui y sont liées - respects des coûts, des délais, du cahier des charges et du niveau de qualité[3].

Il existe plusieurs référentiels de certification du système de management de la qualité en entreprise, en matière d'ingénierie du logiciel comme TickIT.

Indicateurs de qualité logicielle

La norme ISO 9126 définit six groupes d'indicateurs de qualité des logiciels[4] :

- la capacité fonctionnelle. c'est-à-dire la capacité qu'ont les fonctionnalités d'un logiciel à répondre aux exigences et besoins explicites ou implicites des usagers. En font partie la précision, l'interopérabilité, la conformité aux normes et la sécurité ;
- la facilité d'utilisation, qui porte sur l'effort nécessaire pour apprendre à manipuler le logiciel. En font partie la facilité de compréhension, d'apprentissage et d'exploitation et la robustesse - une utilisation incorrecte n'entraîne pas de dysfonctionnement ;
- la fiabilité, c'est-à-dire la capacité d'un logiciel de rendre des résultats corrects quelles que soient les conditions d'exploitation. En font partie la tolérance aux pannes - la capacité d'un logiciel de fonctionner même en étant handicapé par la panne d'un composant (logiciel ou matériel) ;
- la performance, c'est-à-dire le rapport entre la quantité de ressources utilisées

(moyens matériels, temps, personnel), et la quantité de résultats délivrés. En font partie le temps de réponse, le débit et l'extensibilité - capacité à maintenir la performance même en cas d'utilisation intensive ;

- la maintenabilité, qui mesure l'effort nécessaire à corriger ou transformer le logiciel. En font partie l'extensibilité, c'est-à-dire le peu d'effort nécessaire pour y ajouter de nouvelles fonctions ;
- la portabilité, c'est-à-dire l'aptitude d'un logiciel de fonctionner dans un environnement matériel ou logiciel différent de son environnement initial. En font partie la facilité d'installation et de configuration dans le nouvel environnement.

Chaque caractéristique contient des sous-caractéristiques. Il y a 27 sous-caractéristiques.

Les différents indicateurs sont parfois conflictuels, ou au contraire complémentaires : une augmentation de la capacité fonctionnelle peut avoir un impact négatif sur la performance, la maintenabilité et la fiabilité. Tandis qu'une augmentation de la fiabilité, la maintenabilité ou de la disponibilité ont un impact positif sur l'utilisabilité. En outre, une augmentation de la maintenabilité peut avoir un impact négatif sur la performance[5].

Crise du logiciel

Un phénomène de baisse des prix du matériel informatique et d'augmentation des prix du logiciel, accompagné d'une baisse de la qualité des logiciels a été identifié à la fin des années 1960 et nommé la « crise du logiciel ». Cette crise s'apparente aujourd'hui à une maladie chronique de l'industrie du logiciel, dont les symptômes sont les suivants :

- les délais de livraison des logiciels sont rarement tenus, le dépassement de délai et de coût moyen est compris entre 50 et 70 % ;
- la qualité du logiciel correspond rarement aux attentes des acheteurs, le logiciel ne correspond pas aux besoins, il consomme plus de moyens informatiques que prévu, et tombe en panne ;
- les modifications effectuées après la livraison d'un logiciel coûtent cher, et sont à l'origine de nouveaux défauts. Les adaptations sont bien souvent une nécessité du fait de l'évolution des produits et des attentes des utilisateurs ;
- il est rarement possible de réutiliser un logiciel existant pour en faire un nouveau produit de remplacement ; l'amortissement du coût de développement initial est ainsi rendu impossible[6].

Auparavant minoritaire, le coût du logiciel en 1965 représentait 50 % du coût total d'un système informatique. En 1985 la part du logiciel est de 80 % et les coûts dus à la correction des défauts dans les logiciels (maintenance) représentent jusqu'à trois quarts du coût total d'acquisition, un excédent dû uniquement à la mauvaise qualité du logiciel lors de sa livraison.

Selon une étude réalisée en 1994 par le *Standish Group*, 53 % des logiciels créés sont une réussite mitigée : le logiciel est opérationnel, cependant le délai de livraison n'a pas été respecté, les budgets n'ont pas été tenus, et certaines fonctionnalités ne sont pas disponibles. Le dépassement des coûts est en moyenne de 90 %, et celui des délais de 120 %, et la qualité moyenne est estimée à 60 %[7].

Raisons du manque de qualité des logiciels

Un logiciel étant un produit immatériel, les seules représentations observables du logiciel sont le code source, l'interface utilisateur et la documentation (spécification, cahiers de

tests, manuels utilisateur, etc.). La quantité de code source (nombre de lignes) est rarement connue à l'avance, ce qui entraîne souvent une sous-estimation de la complexité du logiciel.

Pour chaque module d'un logiciel il existe de nombreuses conditions d'utilisation. La combinaison des différentes conditions d'utilisation des différents modules d'un logiciel amène une explosion combinatoire, et lors de sa construction, un logiciel n'est jamais contrôlé dans la totalité des conditions d'utilisation qu'il rencontrera durant son exploitation; ceci pour des raisons pratiques (coût et durée des travaux).

Une autre raison est qu'il n'y a pas de lien entre un défaut mineur et majeur, et une modification mineure ou majeure. Et l'effort de détérioration d'un logiciel n'est pas proportionnel à l'effort de construction. Un défaut mineur peut entrainer un incident majeur, et nécessiter une correction mineure. Dans l'incident du vol 501 d'Ariane 5, une correction mineure aurait suffi à éviter la destruction de la fusée. De même une modification mineure d'un logiciel peut le mettre hors d'usage; un phénomène largement exploité par les virus informatiques[8].

Pour être considéré comme produit de qualité par l'usager, un logiciel doit répondre aux besoins exprimés explicitement par l'usager aussi bien qu'aux besoins implicites (non exprimés). Or les vœux implicites évoluent avec le marché, et il arrive bien souvent que des vœux implicites des usagers ne soient pas connus des ingénieurs logiciels[9].

Amélioration de la qualité

En génie logiciel, la factorisation des données et du code constituent le moyen universel d'obtention de la qualité. La factorisation des données aboutit au modèle objet (avec usage de l'héritage) dont le correspondant systématique relationnel est idéal lorsqu'il est normalisé (formes normales de Codd). En effet, lorsque les structures de données sont ainsi normalisées, elles deviennent non redondantes, donc minimales en taille, et n'engendrant aucun problème d'incohérence dès lors que l'intégrité découlant de leur type et l'intégrité référentielle sont assurées, contraintes auxquelles il faut ajouter des "règles métiers" consistant en contraintes logiques faisant intervenir plusieurs champs/attributs. Ce travail au niveau des données permet en soi la réduction du code de traitement exploitant ces données. La performance n'en souffre pas si les requêtes sont bien organisées.

Concernant le code, la factorisation permet de n'écrire qu'une fois des instructions similaires, par un usage raisonné des variables intermédiaires et locales, des boucles, des fonctions et des procédures. Cela permet la réduction maximale de la taille du code source (sans perte normalement de lisibilité), et aboutit à ce que les modifications soient le plus locales possibles (donc plus rapides, et plus fiables en termes de non régression). Un gain complémentaire de réduction du code source est apporté par le polymorphisme et la liaison dynamique (qui éliminent les « procédures aiguillage ») en programmation objet (celles-ci sont générées par le compilateur au lieu de devoir être écrites explicitement par le programmeur). Ces factorisations font émerger les bonnes abstractions, la bonne structuration, et permettent le meilleur contrôle possible de l'intégrité des données et de la bonne exécution des traitements, dont les fonctions, appelées en plusieurs points du code source peuvent devenir de fait des services réutilisés, autant que les données qui, étant partagées, sont réutilisées sans duplication. Ce travail permet à une application d'être "modulaire". Ces modules sont les services. Leur interface étant claire et sans effet de bord, le traitement qu'ils réalisent devient caché (boîte noire) pour ses modules clients. Le couplage entre un module et ses modules appelants devient le plus faible possible, du fait que seules les valeurs de paramètres variant d'un appel à l'autre sont passées en

argument, les variables invariantes entre appels devant idéalement constituer des attributs d'une classe porteuse, la fonction/module en devenant une méthode (dans une programmation objet aboutie). En ce sens, on peut parler de couplage faible, et l'on peut substituer une implémentation à une autre. Il est faux en général que l'on obtienne ainsi la minimisation de l'impact de la défaillance d'un module sur les autres modules et sur le fonctionnement de l'application. La fiabilité y gagne cependant en ce qu'en ayant factorisé, la maintenance du module deviendra un sujet critique à traiter et donc objet d'attentions, la modification restant par ailleurs locale donc plus facilement adressable sans générer de régressions. Pour les modules les plus critiques, leur disponibilité sans faille peut reposer sur une stratégie de redondance d'instanciation physique, ou au contraire le maintien d'une unicité mais sur base d'un service matériel géré de manière autonome par une équipe dédiée. Dans le corps humain, la stratégie adoptée pour les fonctions de l'ouïe, de la vue, de la préhension et du filtrage du sang est la redondance matérielle, alors que celle prise pour l'estomac, le foie, le cœur, le cerveau, la digestion, qui sont tout aussi critiques, est l'unicité du service, mais avec une forte autonomie de gestion.

En jargon de programmation, le syndrome du plat de spaghettis désigne un logiciel de mauvaise qualité au couplage trop fort et au code source difficile à lire, dans lequel toute modification même mineure demande un intense travail de programmation. Le langage de programmation BASIC utilisant la fonction GOTO est couramment pointée comme l'origine de la "mauvaise éducation" des programmeurs formé dans les années 80.

L'abstraction vise à diminuer la complexité globale du logiciel en diminuant le nombre de modules et en assurant l'essentiel. Elle peut également apporter une uniformité du logiciel qui augmente son utilisabilité en facilitant son apprentissage et son utilisation.

La dissimulation vise à séparer complètement les détails techniques du logiciel de ses fonctionnalités selon le principe de la *boîte noire*, en vue d'améliorer sa maintenabilité, sa portabilité et son interopérabilité.

La structuration des instructions et des données rend clairement visibles dans le code source les grandes lignes de l'organisation des instructions et des informations manipulées, ce qui améliore sa maintenabilité et facilite la détection des bugs[10].

De nombreux langages de programmation soutiennent, voire imposent l'écriture de code source selon les principes de structuration, de modularité et de dissimulation. C'est le cas des langages de programmation structurée et de programmation orientée objet.

Notes et références[modifier | modifier le code]

1. ↑ Alain April et Claude Laporte, *Assurance qualité logicielle 1: concepts de base*, Lavoisier, 2011, (ISBN 9782746231474), page 387
2. ↑ Carl-August Zehnder, *Développement de projet en informatique*, PPUR presses polytechniques - 1990, (ISBN 9782880741723), page 174
3. ↑ Marylène Micheloud et Medard Rieder, *Programmation orientée objets en C++: Une approche évolutive*, PPUR presses polytechniques, 2002, (ISBN 9782880745042), page 259
4. ↑ Jean Menthonnex - CERSSI, *Sécurité et qualité informatiques: nouvelles orientations*, PPUR presses polytechniques - 1995, (ISBN 9782880742881), page 77
5. ↑ (en) Stephen H. Kan, *Metrics and models in software quality engineering*, Addison-Wesley - 2003, (ISBN 9780201729153)
6. ↑ « Cycle de vie du logiciel » [archive]
7. ↑ « La crise du logiciel » [archive]
8. ↑ Jacques Perrin, *Conception entre science et art: regards multiples sur la conception*, PPUR presses polytechniques - 2001, (ISBN 9782880744809), page 62
9. ↑ Philippe Dugerdil, *Impact des décisions informatiques: Introduction à l'informatique pour décideur non informaticien*, PPUR presses polytechniques - 2005, (ISBN 9782880746100), page 201
10. ↑ « Introduction au génie logiciel » [archive]

Gestion des risques d'un projet

Un article de Wikipédia, l'encyclopédie libre.

Spécificités d'une organisation de projet

Un projet présente le plus souvent la double caractéristique de se dérouler suivant un processus défini pour l'occasion, et d'avoir une organisation et des objectifs qui évoluent très fortement dans le temps avec l'avancement du projet. De ce fait, une part importante des risques est liée à l'organisation elle-même et au bon déroulement de ses différentes tâches.

Par rapport à une gestion des risques « classique », la gestion des risques d'un projet reflète cette originalité :

- Les niveaux de risque étudiés sont généralement élevés, parce que l'occurrence d'événements imprévus étant une quasi certitude, la gestion des risques faibles serait de toute manière une perte de temps.
- Les événements redoutés sont souvent les mêmes d'un projet à l'autre : mauvaise expression du besoin, défaillance ou indisponibilité d'une ressource, dérapage financier et calendaire, spécification non tenue.
- La gestion du risque consiste le plus souvent à modifier la planification du projet, ou à se préparer à le faire
- Elle tend à être une fonction opérationnelle (contrairement à une gestion des risques classique, plutôt fonctionnelle et transverse).
- Elle peut généralement se contenter d'une approche purement qualitative en ce qui concerne les probabilités d'occurrence, mais demandera souvent une analyse beaucoup plus poussée en termes d'impacts financiers et calendaires.
- Elle est généralement modulaire, chaque sous-traitant étant responsable de sa partie et de ses marges ; ce qui entraîne des problèmes de coordinations spécifiques.

L'évaluation des risques est une analyse approfondie des scénarios éventuels de leur apparition. Elle a pour but de[1] :

- Adopter les mesures adéquates face à ces risques
- Améliorer la sécurité du projet
- Être une base pour la gestion du projet (la planification, l'abandon de certaines fonctionnalités, le choix des fournisseurs, la prévision des délais de livraison et des délais d'adaptation...)

La gestion des risques consiste à s'assurer que tous les risques importants sont maîtrisés. Pour ne pas oublier de traiter un risque on procède à leur recensement. La synthèse du recensement est le tableau de bord des risques du projet.

Analyse des risques

Incertitudes de planification

Une partie de l'incertitude sur le projet vient d'une planification peu détaillée. Initialement, l'estimation des coûts et délais nécessaires pour des activités se situant à une échéance lointaine s'appuie généralement sur un estimateur de coût ; ce n'est que par la suite du projet que sa planification passera progressivement au stade d'un avant-projet plus précis ; et les coûts et délais de référence ne sont définitivement arrêtés qu'après que les différentes tâches aient été effectivement négociées et contractualisées.

L'incertitude sur les coûts et les délais, due à une planification initialement peu détaillée, conduit normalement à prendre sur les différentes tâches des marges calendaires et budgétaires suffisantes pour que l'organisation du projet ne soit pas remise en cause par de petits écarts. Ces marges sont prises par rapport au temps et budget moyens que l'on estimerait nécessaires pour la tâche, estimation qui repose sur l'état du marché et l'expérience de travaux similaires. Théoriquement, ces marges devraient donc en moyenne se solder par des opportunités. Cependant, l'expérience montre que la planification d'un projet est souvent trop optimiste, et même en tenant compte de la loi de Hofstadter, l'effet global de ces incertitudes se traduit le plus souvent par un risque de

dépassement. Un tel risque est par nature difficile à estimer tant que la difficulté réelle n'est pas perçue, puisque son anticipation consisterait précisément à allouer plus de marges lors de la planification.

Ces incertitudes ont cependant une certaine prévisibilité.

- D'une part, le caractère plus ou moins grossier de l'estimation est défini, et les fourchettes d'incertitudes associées sont connues : si un estimateur de coût peut par exemple donner un ordre de grandeur à 50 % près, un avant-projet sommaire fera baisser cette incertitude à 20 %, l'avant-projet détaillé à 5 %, et la contractualisation pourra réduire l'incertitude de planification sous la barre du pour-cent.
- D'autre part, les différentes étapes de planification qui réduiront cette incertitude sont elles-mêmes connues et planifiables.

Il est possible (et le plus souvent souhaitable) d'annoncer au client du projet à la fois l'ordre de grandeur de cette incertitude et la date à laquelle elle sera réduite. De ce fait, même si chaque nouvelle estimation implique un certain risque de constater que l'estimation précédente aura été sous-estimée, ces incertitudes ne relèvent pas réellement de la gestion des risques, mais avant tout d'une bonne maîtrise de la communication avec le client du projet : même si l'engagement contractuel porte sur un chiffre défini, le client doit être conscient de ce qu'un projet comprend toujours une part de marges et d'incertitudes, part qui se réduit au fur et à mesure de l'avancement.

Perception et explicitation

Classification des risques

Suivant qu'ils sont internes ou externes au projet, et qu'ils sont ou non l'objet d'un choix dans la planification du projet, les risques d'un projet peuvent se répartir en quatre grandes catégories[2] :

- Risques externes liés à l'environnement et au contexte (ressources humaines, juridique, stratégique, financier) ;
- Risques externes liés aux sous-traitants (organisation industrielle, contractuel, juridique, qualité, stratégique, économique) ;
- Risques internes associés aux techniques employées (qualité, sûreté, intégrité, expression de besoin, ingénierie système) ;
- Risques internes associés à l'organisation du projet (organisation, gestion des ressources, marges, gestion des risques, qualité interne).

Risques associés à l'organisation du projet

Mauvaise maîtrise des interfaces. Une source constante de risque dans les projets.

Comme signalé ci-dessus, les « événements redoutés » associés à la gestion de projet proprement dite sont assez récurrents, et peuvent être identifiés directement au vu de la planification du projet :

- À toute tâche planifiée avec une date de début et une date de fin correspond un risque calendaire : la tâche peut ne pas pouvoir commencer à la date prévue, ou son déroulement peut prendre plus de temps que prévu. La planification du projet peut faire apparaître un chemin critique, objet d'un suivi plus attentif, mais toute tâche devient critique quand elle s'éternise trop longtemps.
- Du moment que deux sous-projets sont susceptibles d'être en interface, dans leur déroulement ou à travers leurs produits, il y aura un risque d'interface associé (mauvaise coordination calendaire, incompatibilité des choix techniques, ...)..
- Une ressource partagée (installations d'essais, ...) a souvent un calendrier non stabilisé, et peut ne pas être disponible dans le créneau attendu.
- Dès lors qu'une solution choisie par le projet est novatrice ou originale, elle comporte un risque de ne pas atteindre les objectifs qui lui sont assignés, ou de voir surgir des difficultés imprévues. Ce peut être le cas pour un montage organisationnel nouveau, où les acteurs n'ont pas l'habitude de partager une culture commune, ou pour le choix d'une solution technologique dont le niveau de maturité technologique se révèle insuffisant au moment où l'on souhaitait la mettre en œuvre.

- L'expression du besoin par le client (dont ce n'est généralement pas le métier) est le plus souvent imprécise ou peut cacher des éléments implicites. Un dialogue constant sur l'avancement du produit et l'affinage de ses caractéristiques est nécessaire mais souvent non suffisant pour éviter des incompréhensions ou des changements de spécifications.

Risques associés aux tâches du projet

Explosion au décollage d'une fusée Antares dans une mission de ravitaillement de la station spatiale internationale. Certains domaines techniques ne sont pas entièrement maîtrisés, et les tâches qui en dépendent sont à risque.

Par ailleurs, chaque savoir-faire technique dont la mise en œuvre est nécessaire entraîne de son côté des risques à caractère technique (par exemple, s'il faut peindre une pièce, la peinture mal posée peut s'écailler), qui nécessite dans ce domaine technique une compétence suffisante pour spécifier correctement le besoin et contrôler la bonne exécution de la tâche.

Contrairement à la gestion des risques spécifiques du projet, ces risques à caractère technique peuvent le plus souvent être maîtrisés en planifiant des tâches dédiées à caractère technique, de spécification, de contrôle et de recette.

Cette partie de la maîtrise des risques n'est pas spécifique à la gestion du projet, et l'approche pour gérer ces risques propres aux différentes tâches relève des bonnes pratiques du métier correspondant, non de la gestion de projet. Elle n'apparaît dans ce cadre que dans la mesure où les risques d'origine technique peuvent être mal maîtrisés, et avoir des conséquences - notamment en termes de coût et de délais supplémentaires - impactant le projet lui-même.

Appréciation des risques

Une description qualitative des risques est généralement suffisante dans la conduite de projet.

L'analyse de risque d'un projet pourra le plus souvent se contenter d'une grille de probabilité à trois niveaux (>10 %=possible, 10 à 1 %=incertain, <1 %=envisageable) et une grille de conséquences à trois niveaux (A=remise en cause du projet même, B=contrat non respecté, C=gérable avec les marges disponibles). Pour une gestion plus « fine », une grille 5x5 (comportant deux valeurs intermédiaires) peut être préférable.

En effet, la conduite d'un projet est par nature pleine d'imprévus, il ne sert donc à rien de se préoccuper de scénarios très improbables, sachant que les hasards du projet conduiront de toute manière à en modifier la planification longtemps avant que quoi que ce soit d'« improbable » n'ait eu le temps de survenir. Pour les mêmes raisons, les classes de risques et de conséquences peuvent être larges, dans la mesure où l'information nécessaire est ici surtout qualitative.

Pour une méthode purement comptable la démarche va consister a séparer les risques en non-probabilisable et probabilisables. Pour les probabilisable, on va en profiter pour les catégoriser, via des approches avancées ou élémentaires comme l'AMDEC et le diagramme de Farmer. Cela consiste à définir les niveaux de risque, suivre les évolutions de niveau de risque et les éventuels nouveaux risques apparus lors de la réalisation du projet afin de prioriser les actions à mener pour la mitigation des risques[3], c'est une aide à la prise de décision du chef de projet, de son responsable hiérarchique, des auditeurs, des managers des risques, de la direction et éventuellement des juges ou de la haute autorité chargée de l'administration du secteur métier concerné si elle existe.

Gestion des risques

La première évaluation des risques sur la grille probabilité × conséquence va permettre de répartir les risques en fonction de leur gestion, qui peut le plus souvent se limiter à trois ou quatre niveaux :

- Les risques les plus importants font l'objet d'une planification plus approfondie et sont suivis cas par cas, au niveau de la direction de projet.
- Les risques de niveau intermédiaire font l'objet d'un suivi générique : le suivi des indicateurs d'avancement (dépenses, pourcentage d'avancement, coût à terminaison, date prévue d'achèvement, ...) permet de détecter d'éventuels problèmes dans l'exécution d'une tâche, et une veille générale suffit à assurer que si un montage industriel devient irréaliste un montage alternatif reste possible.
- Les tâches situées sur le chemin critique, ou qui n'ont que peu de marge temporelle, peuvent cependant faire l'objet d'un suivi plus attentif.
- Les tâches peu risquées et à faible impact ne nécessitent pas de suivi particulier, même si le suivi par indicateurs d'avancement leur est étendu pour la forme.

Mesures préventives et correctives

Indicateurs d'avancement et mesure de risques

Article détaillé : Diagramme temps-temps.

En gestion de projet, les indicateurs d'avancement sont un instrument de réduction de risque important, qui permet de détecter assez tôt qu'une tâche rencontre des problèmes d'exécution qui risquent de désorganiser le projet. Ce signal d'alerte permet donc d'en prévoir les conséquences et d'étudier les alternatives avant de se trouver devant le fait accompli. Les indicateurs se répartissent en deux grandes catégories : ceux qui suivent la progression physique, et ceux qui suivent la progression financière. Ces différents types d'indicateurs sont complémentaires et doivent être suivis en parallèle, des signaux d'alerte pouvant se manifester d'un côté mais pas de l'autre.

- Un simple suivi d'exécution budgétaire est évidemment insuffisant comme signal d'alerte. De toute évidence un écart entre dépenses et budget traduit un problème d'exécution, mais inversement, il est souvent facile pour un responsable de tâche peu scrupuleux de ne pas s'écarter de son budget alors même que son activité plonge dans le chaos. Un « suivi » financier n'éclaire que le fait accompli, et doit impérativement être complété par un indicateur technique fiable.
- L'écart de progression par rapport à l'avancement temporel de référence est un indicateur d'avancement simple, mais pour des tâches simples : si l'avancement de la tâche est 0 % à la date de début et 100 % à la date de fin trois mois plus tard, l'avancement temporel devrait être de 33 % au bout d'un mois si tout va bien, et de 66 % au bout de deux mois. Le responsable de la tâche doit évaluer son avancement, et estimer d'une manière ou d'une autre que « la tâche est dans l'état que l'on attendait à telle date ». Cette estimation, possible pour une progression essentiellement linéaire, devient évidemment très arbitraire quand la tâche ne se déroule pas comme prévu.

Une ré-estimation périodique du coût à terminaison et de la date prévue d'achèvement permettent de contourner cet inconvénient, et suivre de manière réaliste l'exécution d'un sous-projet d'organisation plus complexe. Ces indicateurs sont cependant d'un emploi délicat, parce qu'ils impliquent que le responsable du sous-projet dévoile tout ou partie de ses marges financières et/ou calendaires. Sur ce plan, la date prévue d'achèvement présente moins de difficulté.

Par accord entre le responsable du projet et celui du sous-projet, la date prévue d'achèvement peut être par exemple définie comme la date de livraison que le responsable du sous-projet s'engage à ne pas dépasser, avec une probabilité de (par exemple) 80 % de tenir cet engagement, compte tenu des aléas susceptibles d'être encore rencontrés sur son sous-projet. Cet engagement inclut de toute évidence des marges calendaire que le responsable du sous-projet se réserve pour gérer une part « normale » d'aléas, mais ces marges sont inconnues du responsable du projet d'ensemble (et doivent le rester). Au fur et à mesure de l'avancement du sous-projet, les aléas se réduisent dans un sens ou dans l'autre, et tendent à se rapprocher de l'estimation moyenne. Le plus souvent, quand le sous-projet se déroule bien, une marge calendaire jugée initialement nécessaire se révèle donc surestimée, et le pari à 80 % peut normalement être progressivement réajusté à une date plus proche. L'avancement normal d'un tel indicateur est donc de le voir progressivement s'avancer - l'absence d'avancement étant probablement le signe que la date n'a pas été réévaluée, ou que le responsable du sous-projet est réticent à rendre ses marges. Inversement, si une difficulté est rencontrée dans le sous-projet, elle conduit à consommer de la marge, voire - si la difficulté est importante - à annoncer un recul dans la date prévue d'achèvement.

De ce fait, le diagramme temps-temps, qui décrit l'évolution des dates prévues pour les principaux jalons d'un projet, est un outil indispensable au suivi des projets complexes.

Un indicateur sur le coût à terminaison d'un sous-projet est similaire dans son principe à celui sur la date prévue d'achèvement. Mais cet indicateur financier présente deux différences importantes, qui le rendent beaucoup moins transparent que le précédent. D'une part, une date d'achèvement peut généralement être avancée sans perturber l'économie du projet ; mais quand un sous-projet rend des marges sur le plan financier, ces marges supplémentaires sont le plus souvent l'objet d'arbitrages internes au projet, et sont finalement consommées ailleurs. D'autre part, contrairement à une date d'achèvement dont le résultat final peut être constaté par tous, un coût ne se confond pas nécessairement avec un prix. Si le sous-projet est confié à un sous-contractant, la marge financière participe de la marge bénéficiaire, et il est impossible dans ce cas d'assigner au coût à terminaison une autre valeur que la valeur contractuelle. De ce fait, cet indicateur ne peut guère refléter dans ce cas que l'état des renégociations contractuelles.

Risques sur les tâches du projet

On ne change pas d'attelage au milieu du gué. En cas de difficulté, changer d'équipe ne fait souvent que rajouter au problème.

Lorsqu'une tâche particulière apparaît comme une source de risque, la principale mesure de réduction de risque consiste à la confier à un opérateur dont la maîtrise est démontrée, même si cela conduit à des surcoûts. À défaut, l'organisation interne du projet peut planifier d'y consacrer plus de personnel, ou une surveillance plus suivie.

Mais le traitement de ce point de faiblesse doit être anticipé ; l'expérience montre que quand une tâche s'avère défaillante, modifier son équipe exécutante en cours de tâche revient à vouloir « changer d'attelage au milieu du gué » : le changement de portage est en soi un facteur de risque, dont l'effet est souvent pire que la dérive en coûts et délais attendue avec l'équipe initiale.

Si dans son déroulement une tâche se déroule mal, l'effet le plus probable est un dérapage des coûts (l'exécution coûte plus cher que prévu) ou des délais (le délivrable n'est pas au rendez-vous attendu). Dans ce cas, la planification calendaire et financière du projet sera remise en cause, dans une mesure qui peut être supportable - ou pas.

L'effet le plus contraignant sur l'organisation du projet est pour une tâche de ne pas atteindre l'objectif attendu. Le produit de la tâche peut néanmoins remplir un certain service, et il reste possible d'utiliser ce résultat « en mode dégradé ». La question devient alors de savoir s'il est possible d'accepter ce surcoût ou ce délai supplémentaire, ou d'utiliser ce résultat dégradé dans le reste du projet.

L'alternative est que le projet doit être réorganisé d'une manière ou d'une autre pour atteindre son but. La matière propre de la gestion d'un projet est la gestion de l'organisation et des risques ; lorsqu'un risque mal maîtrisé conduit à une impasse avérée ou prévisible sur une voie particulière, l'action correctrice consiste à en réorganiser la planification pour passer sur un « plan B » qui permettra de contourner la difficulté et d'atteindre les objectifs.

Gestion des « plans B

D'une manière générale, un changement de référence par rapport à l'organisation initiale est par lui-même un risque, qui entraîne des surcoûts, des incertitudes et généralement des délais, et ceci d'autant plus que le changement dans les plans est tardif et aura été mal préparé. En amont, la mesure préventive de réduction des risques consiste donc en premier lieu à préparer des « plans B » pour faire face aux principaux risques, c'est-à-dire envisager le plus en amont possible des alternatives crédibles et fiables à la planification de référence.

Si la conduite d'un projet « sur les rails » par rapport à sa planification peut être comparé à assurer la progression d'un train sur son itinéraire de référence, l'activité de gestion des risques consiste alors à s'assurer en permanence de l'état réel des voies qui doivent être parcourues, à identifier des itinéraires alternatifs, et à faire basculer si nécessaire les aiguillages sur les « plans B » avant que le train n'y soit passé - un retour en arrière est toujours plus coûteux qu'un branchement sans heurt sur une dérivation.

La maîtrise des « plans B » ne se limite pas toujours à leur simple planification. Dans certains cas, la solution alternative suppose que certaines dispositions soient prises en amont à titre conservatoire, et que certaines tâches soient lancées ou réalisées le long de la « planification B », pour préparer le terrain, avant même de savoir si le basculement sera effectivement nécessaire. De même, des études peuvent être nécessaires pour évaluer correctement le risque de la planification de référence : un démonstrateur peut valider une technologie innovante avant d'engager sa mise en œuvre en vraie grandeur. Dans ce cas, les dispositions conservatoires et les tâches anticipées constituent autant de mesures préventives de réduction de risque : elles n'empêchent pas l'événement redouté, mais en diminuent l'impact si le passage au « plan B » devient nécessaire.

Inversement, si tout se passe bien sur la planification de référence, ces tâches de réduction de risque seront arrêtées sans suite, le moment venu.

Impact des risques sur les coûts et les délais

Dans les cas simples, les « événements redoutés » sur une tâche sont directement exprimés au niveau du projet sous la forme de dépassements de délais ou de budget. En effet, un risque à caractère technique se traduit le plus souvent avant tout par un délai supplémentaire nécessaire pour corriger le défaut, et éventuellement par un surcoût de la tâche (quand elle n'est pas exécutée forfaitairement). L'impact de tels risques sur le projet dans son ensemble se réduit alors à savoir si ces dépassements peuvent être absorbés dans les marge encore disponibles (auquel cas ils seront transparents pour le client du projet), ou s'ils entraîneront un dépassement par rapport aux objectifs d'ensemble du projet.

Dans des cas plus complexes, où des planifications alternatives sont nécessaires, c'est cette planification même qui permet de déterminer l'impact du risque sur le projet. L'effet du risque étant de passer d'un « plan A » à un « plan B », son impact correspond à la différence entre ces deux planifications. Il faut cependant noter que dans ce cas, d'éventuelles mesures conservatoires ou actions de réduction de risque font partie de la planification de référence, bien qu'elles soient justifiées par le risque qu'elles réduisent. D'autre part, les tâches du « plan A » qui en fin de compte ne seront pas exécutées n'ont pas nécessairement pour autant un coût nul : elles ont demandé un certain travail de préparation, et certains travaux préparatoires ou certains contrats ont pu être engagés avant que la décision de changer le plan de référence n'ait été prise.

1. ↑ http://www.secinfo.gouv.fr/gp_article50.html [archive]
2. ↑ Analyse des risques projet [archive], G.Claverie - CNRS Ecole Projet IN2P3 – novembre 2012
3. ↑ Gestion des risques d'un projet - Les Techniques de l'Ingénieur - Référence SE2040 - Date de publication : 10 oct. 2008 - Alain DESROCHES [archive]

Sécurité : Sécuriser les sites web

S’assurer que les bonnes pratiques minimales sont appliquées aux sites web.

Tout site web doit garantir son identité et la confidentialité des informations transmises.

Les précautions élémentaires

Mettre en œuvre **le protocol TLS** (en remplacement de SSL) sur tous les sites web, en utilisant uniquement les versions les plus récentes et en vérifiant sa bonne mise en œuvre.

Rendre l’utilisation de TLS obligatoire pour toutes les pages d’authentification, de formulaire ou sur lesquelles sont affichées ou transmises des données à caractère personnel non publiques.

Limiter les ports de communication strictement nécessaires au bon fonctionnement des applications installées. Si l’accès à un serveur web passe uniquement par HTTPS, il faut autoriser uniquement les flux réseau IP entrants sur cette machine sur le port 443 et bloquer tous les autres ports.

Limiter l’accès aux outils et interfaces d’administration aux seules personnes habilitées. En particulier, limiter l’utilisation des comptes administrateurs aux équipes en charge de l’informatique et ce, uniquement pour les actions d’administration qui le nécessitent.

Si des ***cookies* non nécessaires au service sont utilisés, recueillir le consentement** de l’internaute après information de celui-ci et avant le dépôt du *cookie*.

Limiter le nombre de composants mis en œuvre, en effectuer une veille et les mettre à jour.

Ce qu’il ne faut pas faire

- Faire transiter des données à caractère personnel dans une URL telles que identifiants ou mots de passe.
- Utiliser des services non sécurisés (authentification en clair, flux en clair, etc.).
- Utiliser les serveurs hébergeant les bases de données ou des serveurs comme des postes de travail, notamment pour naviguer sur des sites web, accéder à la messagerie électronique, etc.
- Placer les bases de données sur un serveur directement accessible depuis Internet.
- Utiliser des comptes utilisateurs génériques (c’est-à-dire partagés entre plusieurs utilisateurs).

Pour aller plus loin

- Concernant la mise en œuvre de *cookies*, il est conseillé de consulter le dossier « *Site web, cookies et autres traceurs* ».
- S’agissant des logiciels s’exécutant sur des serveurs, il est conseillé d’utiliser des **outils de détection des vulnérabilités** (logiciels scanners de vulnérabilité tels que nmap, nessus, nikto, etc.) pour les traitements les plus critiques afin de détecter d’éventuelles failles de sécurité. Des systèmes de détection et prévention des attaques sur des systèmes ou serveurs critiques peuvent aussi être utilisés. Ces tests doivent être menés de façon régulière et avant toute mise en production d’une nouvelle version logicielle.
- **L’ANSSI a publié sur son site des** **recommandations spécifiques** pour mettre en œuvre TLS ou pour sécuriser un site web.