Démarche d'ingénierie de la sécurité dans le management de projet : activités de sécurité et relations entre acteurs

Wilson Goudalo, Frédéric Vanderhaegen, Christophe Kolski

Atelier "Sécurité des SI : technologies et personnes", Inforsid 2016, INFormatique des ORganisation et Systèmes d'Information et de Décision, Toulouse, France, juin.

Démarche d'ingénierie de la sécurité dans le management de projet : activités de sécurité et relations entre acteurs

Wilson Goudalo [1,2], Christophe Kolski [1], Frédéric Vanderhaegen [1]

1. LAMIH-UMR CNRS 8201, Université de Valenciennes
59313 Valenciennes, France
{wilson.goudalo, christophe.kolski, frederic.vanderhaegen}@univ-valenciennes.fr

2. Research and Innovation Department, ABE - Advanced Business Engineering
77400 Lagny, France
wilson.goudalo@abe-engineering.net

RESUME. *Dans de nombreux cas de projets d'entreprises et d'organisations, la sécurité est juste considérée comme des exigences qui sont prises en compte à la fin des projets et des initiatives, souvent à la mise en production, et parfois pendant la production. Dans de telles situations, il n'y a ni une vision globale de la sécurité, ni un pilotage harmonisé considérant l'ensemble des acteurs. L'application des règles et la mise en œuvre des outils de la sécurité y sont considérées comme une surcouche ou bien des contraintes. Cela cause de nombreux problèmes de sécurité. Par conséquent, des irritants majeurs, des manques à gagner, des problèmes de non-conformité règlementaire à la protection de données personnelles, ou bien des vols et des pertes directes peuvent survenir. Dans ce travail nous proposons de contribuer à l'élaboration d'une ingénierie de la sécurité dans le management de projet, en nous focalisant sur les activités de sécurité et les relations entre les acteurs.*

ABSTRACT. *In many cases of projects, security is just seen as requirements that are taken into account at the end of projects and initiatives, often at the start of production, and sometimes during production. In such situations, there is no overall vision of security, nor harmonized steering with the various actors. The application of rules and the implementation of security tools are seen as an overlay or constraint. This causes countless security issues (resilience, usability, and user experience). Consequently, major irritants, shortfalls, problems of regulatory non-compliance with the protection of personal data, or theft and direct loss could occur. This work aims to contribute to the development of security engineering in the project management; we proposed the security activities and relations between the actors.*

MOTS-CLES : *Sécurité ; Acteurs ; Rôles ; Management de Projet ; Risques de Sécurité.*

KEYWORDS: *Security; Actors; Roles; Project Management; Projects; Security Risks.*

1. Introduction

La sécurité de l'information est définie comme étant la préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information (ISO/IEC 27000). Le périmètre de la sécurité de l'information couvre le stockage, l'accès, le transport et le traitement de l'information. La sécurité de l'information s'applique à la conduite des collaborateurs ainsi qu'aux applications, aux systèmes, aux équipements et aux locaux qui créent, traitent, transmettent, hébergent ou stockent des informations, qu'elles soient internes, personnelles ou fournies par des tiers (EBIOS ANSSI, 2016). L'ingénierie de la sécurité de l'information dans les projets d'entreprise devrait préserver la confidentialité, l'intégrité et la disponibilité de tous les actifs IT, afin de réaliser efficacement les objectifs stratégiques d'entreprise et de garantir sa bonne réputation, de même que sa conformité règlementaire et légale. D'une part, elle devrait faciliter les risques projet, ayant rapport avec l'information, son partage et sa sécurité. D'autre part, elle devrait favoriser l'amélioration continue de la sécurité d'entreprise, en garantissant la prise en compte de la sécurité dans les livrables projets et à chaque étape de leur cycle de vie. Les projets d'entreprise sollicitent la collaboration et la participation de plusieurs acteurs. Les bonnes pratiques de gestion de projets définissent des phases de projets et des acteurs pour chaque phase, afin de fournir les livrables conformes aux attentes.

Dans cet article, nous nous proposons de contribuer à l'élaboration d'une ingénierie de la sécurité qui accompagne les projets d'entreprise dans leurs cycles de vie, avec pour objectif de garantir le succès des livrables et d'éviter les risques projets en termes de sécurité, de dérapage et de non-conformité. Nous nous sommes inspirés d'une part des bonnes pratiques de gestion de projets de PMI, au sein du PM BOK (PMI, 2017),

et d'autre part des récents travaux sur l'ingénierie conjointe de la sécurité, de l'utilisabilité et de la résilience dans les systèmes sociotechniques (Goudalo et al., 2016, 2017). Le présent article est structuré comme suit. Dans la deuxième section, nous présentons un bref état de l'art du management de projets d'entreprise, des enjeux de la sécurité et du respect de la vie privée, et de la prise en compte des risques de sécurité dans le management de projets. Dans la troisième section, nous élaborons la nouvelle ingénierie de la sécurité qui se greffe sur les phases de management de projets et proposons la matrice de RASCI adéquate. Dans la quatrième section, nous illustrons et discutons de notre proposition d'ingénierie. L'article se termine par une conclusion et des perspectives de recherche.

2. Etat de l'art

2.1. Sécurité

La famille des normes ISO 27000 (2016) est dédiée à la sécurité de l'information. Ces normes présentent comment établir, mettre en œuvre, maintenir et améliorer continuellement un système de gestion de la sécurité de l'information. Elles définissent la sécurité en termes de trois concepts fondamentaux : la confidentialité, l'intégrité et la disponibilité des informations, en appliquant un processus de gestion des risques. D'autres normes internationales et locales traitent également la sécurité, ainsi que les risques de sécurité des SI. La communauté des chercheurs industriels et universitaires a effectué récemment différents travaux, répondant aux nouvelles exigences de l'économie numérique (IBM Corporation, 2014), en termes de sécurité, utilisabilité et résilience (Goudalo et al., 2016 et 2017), (European Commission, 2009 et 2013), (ReSIT, 2017).

2.2. Management de projet

ISO 21500 (2012) définit le projet comme un processus unique qui consiste en un ensemble d'activités coordonnées et maîtrisées, comportant des dates de début et de fin, entrepris dans le but d'atteindre un objectif conforme à des exigences spécifiques, incluant des contraintes de délais, de coûts et de ressources.

PRINCE2 (Prince2, 2017) est une méthode anglaise basée sur des processus et qui est communément utilisée à l'international pour un management efficace de projet. Il s'agit de l'acronyme pour « PRojects IN Controlled Environments – Projets en environnements contrôlés ». Selon PRINCE2, le management de projet, tel un ensemble de processus, consiste d'une part à planifier, déléguer surveiller et contrôler les activités relatives à tous les aspects du projet, et d'autre part à motiver les personnes concernées pour atteindre les objectifs du projet dans le cadre des indicateurs de performance attendus par l'organisation ou l'entreprise. Aussi bien que toutes les opportunités doivent être saisies, les risques et les irritants doivent être identifiés et traités à leur juste valeur. PRINCE2 s'appuie sur 7 principes soutenus par 7 thèmes et 7 processus. Il définit les rôles et les responsabilités, la description des produits et l'ordre des activités dans les processus, tout en vérifiant la justification business tout au long du projet. Les 7 processus de PRINCE2 sont : Elaborer le projet, Initialiser le projet, Gérer une limite de séquence, Gérer la livraison de produits, Contrôler une séquence, Diriger le projet et Clore le projet. Les 7 thèmes de PRINCE2 couvrent les disciplines de management de projet qui garantissent son contrôle et qui sont traitées de façon continue tout au long du cycle de vie du projet. Les 7 thèmes définis par PRINCE2 sont : le cas d'affaire, l'organisation, la gestion de la qualité, la planification, la gestion des risques, la gestion des changements, et le contrôle de la progression.

PMI (Project Management Institute), un institut internationalement reconnu, définit le PMBOK (*Project Management Body Of Knowledge* - Corpus des connaissances en management de projet) qui est un cadre de bonnes pratiques à appliquer par le responsable de projet projet (PMI, 2017). PMBOK définit 42 activités et couvre 5 processus qui ont chacun des données d'entrée, des données de sortie, outils et techniques. Les 5 processus de PMBOK : Démarrer, Planifier, Exécuter, Surveiller et Maîtriser, Clôturer. Les processus de PMBOK sont divisés en dix domaines de connaissance (ou disciplines de management) : l'intégration, la portée, le temps, le coût, la qualité, les ressources humaines, les risques, la communication, l'approvisionnement et les parties prenantes. Les domaines de connaissance sont eux aussi définis sous forme de processus ayant chacun des données d'entrée, des données de sortie, activités et techniques.

Dans cette section nous avons montré que le management de risques est commun aux principaux standards internationaux (mondialement reconnus) de management de projet. De même, ils définissent tous un échéancier avec des activités transverses.

2.3. Management de risque dans les projets à l'ère de l'économie numérique

Les standards de management de projet définissent le risque comme un événement incertain ou une condition incertaine qui, si cela se produit, a un effet positif ou négatif sur les objectifs du projet concerné (PMBOK, 2017), (PRINCE2, 2017). Comme nous l'avons démontré dans la section précédente le management de risques est une discipline commune à tous les standards de management de projet. Le « Cas d'affaire » de PRINCE2, qui est essentiel et obligatoire, fait surveiller en permanence la viabilité du projet face aux risques et aux opportunités (PRINCE2, 2017). Dans PRINCE2 la viabilité du projet n'est jamais acquise, elle doit être vérifiée et validée de façon systématique tout au long du projet. De façon intrinsèque, les projets présentent des risques de budget, délai, conformité, sécurité qui menacent les objectifs projets sur les axes de coût, de délai, de performance. Cela est pris en charge par le processus d'analyse et de management des risques de projets. ISO 21500, PRINCE2 et PMBOK basent leurs disciplines de management de risque sur les standards internationaux de management de risque ISO 31000.

A l'ère de l'économie numérique où le digital envahit toutes les sphères de la vie socio-économique, le risque de sécurité devient de plus en plus présent. L'adoption de la sécurité dans les projets, à travers une démarche d'ingénierie présente un avantage majeur pour l'ensemble des parties prenantes. L'ingénierie de la sécurité dans les projets devrait y traiter la sécurité de façon harmonieuse depuis les phases en amont, pendant les phases de construction, pendant les phases d'opération et jusqu'à la phase de clôture. Les travaux de Kolski et ses collègues sur le cycle de développement du logiciel (Kolski et al., 2001) ont mis en évidence l'enrichissement possible de phases des cycles de vie classiques (cascade, V, Spirale…). Les travaux de Goudalo sur la sécurité Business à la Commission Européenne ERCIM (*European Research Consortium for Informatics and Mathematics*) ont mis en évidence les phases d'ingénierie des systèmes d'information au regard de la sécurité (Goudalo, 2008).

En synthèse, nous retenons que le management de projet est effectivement un échéancier de phases séquentielles (contenant des itérations éventuelles) avec une phase transverse. Les phases séquentielles comprendraient : Opportunité, Faisabilité, Conception, Mise en œuvre, Homologation, Exploitation et Clôture. Chaque phase se définit par un objectif majeur et fournit en sortie un ou plusieurs résultats concrets, même si ces derniers sont intermédiaires dans le processus de management de projet. Plusieurs acteurs contribuent à leur réalisation avec différents niveaux de responsabilité et d'implication. Dans la section suivante, notre contribution porte sur la définition des activités de l'ingénierie de la sécurité et les rôles des acteurs au regard des phases de management de projet (PM – Project Management).

3. Contribution

Compte tenu de la place limitée, nous présentons trois extraits de tableaux de notre contribution. Ils portent seulement sur les phases d'étude d'opportunité et d'étude de faisabilité ; ils présentent les acteurs, leurs relations et leurs rôles dans les activités de sécurité sur ces deux phases de PM. Dans la version complète des tableaux, les relations et les rôles des acteurs sur les activités de sécurité sont élaborés au regard de toutes les phases de PM issues des principaux standards de management de projet, mondialement reconnus. Ces tableaux plus exhaustifs pourront être présentés lors de l'atelier.

3.1. Principales activités de l'ingénierie de la sécurité pour le management de projets

On ne saurait garantir la complétude des données, afin d'y appliquer seulement des approches statistiques ou actuarielles. Il ne serait non plus judicieux de se contenter seulement d'une approche intuitive. Des projets pourraient être très sensibles et stratégiques, ils pourraient nécessiter de fortes composantes innovantes, techniques, d'ingénierie, et recourir à de multiples acteurs et parties prenantes. Une démarche systématique d'ingénierie serait opportune pour assurer la sécurité des projets. Dans ce travail nous nous restreignons au seul périmètre du risque de sécurité. Tout risque de sécurité menaçant la réalisation des objectifs du projet doit être identifié, analysé et traité.

A la fin de la section précédente, nous avons retenu les phases suivantes issues du PM : étude d'Opportunité, analyse de Faisabilité, Conception, Mise en œuvre, intégration et Homologation, production et Exploitation, puis Clôture du projet. Dans cette section, nous suggérons des activités d'ingénierie de la sécurité au travers des phases de management de projets, en nous inspirant des travaux d'ingénierie avancée de la sécurité des SI d'entreprise (Goudalo et al., 2016 et 2017). Nous définissons les activités de sécurité dans le Tableau 1.

Qu'il concerne la sécurité, le métier ou le marché, avec toute simplicité (sans rentrer dans aucune complication), le risque se définit par la probabilité d'une perte multipliée par la conséquence d'une perte. A

l'ère de l'économie numérique, il faut identifier les facteurs et sources de risques de sécurité dans le cadre de management de projet. Dans la pratique, on recourt aux check listes, à des interviews et/ou des brainstormings.

Tableau 1. Activités de l'ingénierie de la sécurité dans les phases du PM

Phases de PM	# activités	Activités d'ingénierie de la sécurité
Etude d'opportunité		
	1.1	Identifier les principaux actifs d'entreprise concernés par le projet
	1.2	Définir les valeurs portées par ces actifs et leur sensibilité par rapport au métier de l'entreprise, la réglementation et la législation
	1.3	Analyser à haut niveau les risques au regard des opportunités
Analyse de faisabilité		
	2.1	Définir le périmètre et identifier tous les actifs concernant le projet
	2.2	Préciser le contexte d'utilisation, les scénarios et les responsables associés
	2.3	Identifier les lois, règlements et politiques concernant l'environnement de production cible, et les revoir
	2.4	Procéder à la cotation précise des actifs, en traitant en profondeur le questionnaire MOA/MOE,
	2.5	Définir les rôles et les responsabilités en termes de sécurité
	2.6	Définir les objectifs de sécurité
	2.7	Approfondir l'analyse de risques (enjeux, menaces, probabilité de vraisemblance, impacts) Évaluer l'effet d'une perte si une brèche devait se produire, Evaluer les menaces et les vulnérabilités, Déterminer le risque résiduel et prioriser les risques
	2.7	Préciser des normes de sécurité
	2.8	Élaborer des exigences et spécifications de sécurité et de qualité de services (utilisabilité, résilience, expérience utilisateur)

L'expérience de l'analyse quantitative et qualitative des risques, par leur description, leurs impacts, probabilité de vraisemblance et catégorisation (classification), conduit souvent à 5 ou 10 classes principales de risques qui nécessitent un suivi attentif, en fonction de la nature et du contexte du projet. Il est judicieux de confronter cette analyse au retour d'expériences empiriques, au moyen des outils de bases de connaissances ou des moteurs de statistiques avec intelligence augmentée. En fonction du contexte (écosystème socio-économique et règlementaire), de la sensibilité du projet, de la stratégie des sponsors et dans l'intérêt de l'ensemble des parties prenantes, le traitement de risque nécessiterait de :

- Identifier des mesures préventives afin d'éviter les risques ou d'atténuer leurs impacts ;
- Etablir des plans de contingence pour traiter les risques en cas d'occurrence ;
- Initier des investigations permettant d'améliorer des connaissances sur les risques, afin de réduire les facteurs d'incertitudes ;
- Transférer contractuellement le risque à d'autres parties ;
- Etablir et accepter les risques résiduels.

Cela exige une approche d'amélioration continue et l'adhésion de l'ensemble des parties concernées. Nous présentons notre suggestion relative aux relations entre les acteurs et leurs rôles dans les différentes activités de l'ingénierie de la sécurité dans le management de projet. Pour ce faire, nous recourons au formalisme de RASCI.

3.2. Relations entre les acteurs – Leurs rôles suivant la matrice RASCI

Dans ce travail d'ingénierie de la sécurité dans le management de projet, nous portons une attention particulière aux phases de PM et aux activités de sécurité sous-jacentes. Pour une meilleure organisation dans la collaboration, nous proposons de définir les relations entre les acteurs et parties prenantes, au moyen de la matrice de RASCI, aussi désignée par matrice de RACI ou RACI tout simplement (Clet et al., 2013).

Les rôles définissant les relations

Avant d'élaborer la synergie entre les acteurs, à travers le diagramme de RASCI, nous définissons chacun des rôles imputables.

- Responsable (Responsible), la personne qui réalise l'action ou la tâche proprement dite. Ce rôle peut être partagé, et même, déléguée.
- Approbateur (Accountable), la personne qui approuve et qui porte la responsabilité que l'action ou la tâche est effectivement réalisée. Cette responsabilité ne peut être déléguée. Elle fait office d'autorité à tous les niveaux les plus bas et est impliquée à des niveaux supérieurs.
- Consulté (Consulted), la personne qui est consultée avant la réalisation de l'action ou de la tâche. Ceci implique une communication bidirectionnelle.
- Informé (Informed), la personne qui est informée après la réalisation de l'action ou de la tâche.

Dans le cadre des processus opérationnels et techniques, on y rajoute le rôle du Support et on parle du RASCI. Le RASCI (ou le RACI) est utilisé, afin d'éviter les problèmes fondamentaux avec un processus où des personnes erronées sont impliquées et/ou personne n'en est vraiment responsable.

Les principaux acteurs

Dans ce travail, nous proposons de considérer les acteurs que nous regroupons dans le Tableau 2.

Tableau 2. Acteurs de la sécurité en PM

Identifiant	Désignation de l'acteur	Commentaires / Observations
i.	**Sponsor**	Le représentant des hauts responsables (de l'organisation ou l'entreprise) et des propriétaires des actifs du projet
ii.	**Responsable de l'équipe avant-projet**	Pendant l'étude d'opportunité
iii.	**Chargé de la sécurité du projet**	Responsable risques et sécurité du projet
iv.	**Les autres chargés de … sur le projet**	Chargé d'affaire, Chargé du métier, Chargé de la technologie, Chargé de la conformité sur le projet
v.	**Responsable du projet**	Responsable du management du projet
vi.	Collaborateurs de l'équipe projet	Y compris les experts en sécurité, affaires, technologie, etc. sur le projet
vii.	**Représentants clients**	Y compris les utilisateurs internes et externes
viii.	Responsable de l'organisation ou l'entreprise	Le CEO/DG ou son représentant en fonction de la portée du projet
ix.	Collaborateurs de l'organisation ou l'entreprise	En fonction de la portée du projet
x.	Dirigeants de l'organisation ou l'entreprise	Les cadres dirigeants ou leurs représentants, en fonction de la portée du projet
xi.	Comité de pilotage de la sécurité de l'organisation ou l'entreprise	Le CISO et une équipe transverse, en fonction de la portée du projet
xii.	Comité de pilotage de l'IT de l'organisation ou l'entreprise	Le CIO et une équipe transverse, en fonction de la portée du projet
xiii.	Equipe opérationnelle de sécurité de l'organisation ou l'entreprise	La communauté des opérationnels de la sécurité, fonction de la portée du projet et de l'entreprise

Dans le Tableau 3, nous présentons un extrait des acteurs et des rôles sur quelques activités de l'ingénierie de la sécurité au regard du management de projet.

Tableau 3. Relations et rôles des acteurs de la sécurité en PM

Phases de PM	# Activités Sécurité	RASCI - Rôles de quelques acteurs (par leurs identifiants)					
		i	ii	iii	iv	v	vii
Etude d'opportunité							
	1.1	A	R	S	S		C
	1.2	A	R	S	S		I
	1.3	I	A	R	S	I	C
Analyse de faisabilité							
	2.1	A		S	S	R	I
	2.2	I		R	R	A	S
	2.4	C		R	R	A	S
	2.7	I		R	C	A	I
	2.8	I		R	S	A	C

4. Illustration et discussions

L'ingénierie de la sécurité dans les projets, en plus de la sécurité dans la réalisation des objectifs de projet, apportent une nouvelle visibilité, clarification, transparence et une meilleure organisation dans la collaboration et dans le management de projet, ensemble avec tous les acteurs et les parties prenantes. Les travaux réalisés en vue de la sécurité apportent une meilleure compréhension du projet sur d'autres aspects également, pour l'intérêt de toutes les parties prenantes. Des expériences de management de projets dans les organisations et entreprises respectables, nous rappelons deux chiffres importants. En moyenne, 20% du budget total sont mis en provision pour risques. Une gestion suivie et récurrente des risques exigent une charge moyenne de 5 à 10% du budget total. Plus en amont est menée la gestion du risque, plus raisonnable est la charge de ses activités. Une démarche d'ingénierie de sécurité, débutant dès les phases amont des projets, constituerait un investissement dont les bénéfices socio-économiques seraient importants pour les projets, en termes financiers, délais, satisfaction et expérience utilisateurs pour l'ensemble des parties prenantes.

Les risques de sécurité qui n'ont pas été couverts pendant les phases d'études et de construction de projet exigeront davantage de ressources et de moyens pendant les phases d'opération (production / exploitation). Pendant les phases d'études, notamment en phase de faisabilité, le projet est encore très flexible aux différentes orientations qui amélioreront, en particulier, les risques. Les options d'implémentation, améliorant les risques de sécurité, pourront y être retenues pour le grand bénéfice dans l'optimisation des phases ultérieures. De même, les clients (utilisateurs finaux représentés par l'acteur vii), les sponsors et les acteurs internes et externes du projet pourront partager les résultats d'analyse de risques de sécurité et le suivi de leur gestion. Des décisions avisées seront prises à temps opportuns avec une meilleure compréhension. Les termes de la relation avec les fournisseurs devront être définis à bon escient. D'une part, cela devrait optimiser les tâches de réalisation et d'autre part faciliter les tâches en phases d'opération et d'exploitation, pour une meilleure expérience utilisateur. Comme indiqué en début de la section 3, nos travaux s'étendent au-delà des phases d'Etude d'opportunité, et

d'Analyse de faisabilité. Pour les phases de Conception, Mise en œuvre, Homologation, Exploitation et Clôture de projet, nous avons défini une vingtaine d'activités de sécurité supplémentaires.

Bien que le risque zéro n'existe pas, quand l'ingénierie de la sécurité est bien menée dans le management de projets, elle devra garantir la performance attendue des projets en phases d'exploitation, en termes d'indicateurs socio-économiques. Les grands projets, les projets d'innovation, les projets recourant à de nouvelles technologies, les projets sensibles (conformité, opérations critiques, importants cash-flow) devraient bénéficier d'une telle ingénierie, mais encore plus enrichie.

5. Conclusion et perspectives

Dans notre proposition, nous nous sommes inspirés des travaux d'ingénierie avancée de la sécurité et recentrés sur le formalisme du RASCI, au regard des standards internationaux de management de projet. Le RASCI favorise le travail collaboratif et la synergie entre les différents acteurs, aussi hétérogènes qu'ils puissent être. Par clarification des rôles et des responsabilités, chaque acteur est impliqué à sa juste valeur pour assumer la responsabilité adéquate au bon moment. Les doublons d'effort, les mauvaises compréhensions et la prise de mauvaises décisions sont réduites. Au même moment, la clarification des périmètres, la communication et les vues multifonctionnelles sont améliorées pour l'ensemble des parties prenantes. Le débat actuel de la sécurité de l'information s'articule autour du retour sur investissement.

Avec des éléments d'évaluation, il pourra être bénéfique d'analyser les aspects économiques de cette approche d'ingénierie, en termes de coût et de valeur ajoutée au regard de la productivité, de la qualité des livrables et de la satisfaction des acteurs. Une comparaison avec les résultats de gestion de projet, sans l'accompagnement de l'ingénierie de la sécurité, sera opportune. Telles sont les pistes de réflexion de nos futurs travaux, afin d'affiner notre démarche d'ingénierie de la sécurité. Nous envisageons aussi de définir un canevas avec ses étapes importantes, afin de définir une ingénierie de la sécurité qui fera considérer la cyber-sécurité de façon intrinsèque dans le management des projets socio-économiques, à l'ère de l'économie numérique.

Bibliographie

Clet E., Maders H.P., Leblanc J., Goldfarb M. (2013), "Le métier de chef de projet", Editions Eyrolles, novembre 2013, Paris

EBIOS ANSSI, (2016). EBIOS - Expression des Besoins et Identification des Objectifs de Sécurité, https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/ [Dernier accès en septembre 2016]

European Commission, (2009). "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"', COM (2009) 149 final (2010/C 255/18)

European Commission, (2013). "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace". JOIN (2013) 1 final.

Goudalo W., Kolski C., Vanderhaegen F. (2017). Vers une Ingénierie Avancée de la Sécurité des SI d'entreprise : une approche conjointe de la sécurité, de l''utilisabilité et de la résilience dans les systèmes sociotechniques. Ingénierie des Systèmes d'Information, sous presse.

Goudalo W., Kolski C., Vanderhaegen F. (2016). Vers une ingénierie conjointe de la sécurité, de l''utilisabilité et de la résilience dans les systèmes socio-techniques. Atelier "Sécurité des SI : technologies et personnes", Inforsid 2016, INFormatique des ORganisation et Systèmes d'Information et de Décision, Grenoble, France, juin.

Goudalo, (2008). "Business Security", Processed in ERCIM 2008 - European Research Consortium for Informatics and Mathematics, Ressource Internet https://www.ercim.eu/images/stories/seminar1/Panel1-WilsonGoudalo.pdf [Dernier accès en avril 2017].

IBM Corporation, (2014). "Understanding big data so you can act with confidence". Produced in USA, Copyright IBM Corporation, June 2014.

ISO 21500:2012, Lignes directrices sur le management de projet

ISO/IEC 27000:2016, Technologies de l'information -- Techniques de sécurité -- Systèmes de gestion de sécurité de l'information

ISO 31000:2009, Management du risque -- Principes et lignes directrices

Kolski C., Ezzedine H., Abed M. (2001). Développement du logiciel : des cycles classiques aux cycles enrichis sous l'angle des IHM. In Kolski C. (Ed.), Analyse et Conception de l'IHM. Interaction Homme-machine pour les SI, vol. 1, Hermès, Paris, pp. 23-49.

PMI, (2017). "PMBOK - Project Management Body Of Knowledge", Ressource Internet https://www.pmi.org/ [Dernier accès en avril 2017].

PRINCE2, (2017). "PRINCE2 processes and how they fit together", Ressource Internet https://www.prince2.com/ [Dernier accès en avril 2017].

ReSIST, (2017). "Resilience for Survivability in IST". http://www.resist-noe.org/ [Dernier accès en avril 2017].