# Systématisation d'une Démarche de Sécurisation par Conformité Ajustée aux Besoins et Enjeux de Sécurité – une Revue Critique

Stéphane Paul[a], Nicolas Van Cauter[b], Paul Varela[b], Simon Leboeuf[c] et Michael Catroux[c]

[a] *Thales Research & Technology, 1 avenue Augustin Fresnel, 91767 Palaiseau cedex, France*
[b] *Thales SIX GTS France, 4 avenue des Louvresses 92230 Gennevilliers cedex, France*
[c] *Thales Services Numériques, Mérignac 33700, France*

**Résumé**

Les approches pour sécuriser un système se sont longtemps organisées en deux camps. Le premier camp privilégiait une étude de la conformité vis-à-vis de référentiels génériques. L'autre camp privilégiait l'étude exhaustive de scénarios de risque en tant qu'outil support à la prise de toute décision de sécurisation. Cependant, ces approches ont montré leurs limites. L'étude par conformité est simple, mais ne colle pas forcément aux besoins et enjeux. L'étude par scénarios est exhaustive et spécifique, mais laborieuse, pour au final proposer un bon nombre de mesures de sécurité classiques. Suite à ce constat, des approches hybrides sont apparues : d'abord une étape de sécurisation par conformité, plus ou moins ad-hoc, propice à une certaine automatisation, puis une étape d'analyse par scénarios, manuelle et à dire d'expert, pour compléter le socle de mesures, si nécessaire. Ces approches hybrides rebattent les cartes d'un point de vue sociétal et d'organisation du travail. Les ingénieurs et architectes généralistes prennent l'initiative sur certaines activités de cybersécurité, libérant de fait du temps pour les experts, qui peuvent se concentrer sur des activités à haute valeur ajoutée. Cependant, le premier niveau de sécurisation par conformité reste une opération globalement mal maîtrisée qu'une automatisation pourrait simplifier. Ce papier effectue une revue critique des normes et standards actuels qui proposent cette approche hybride. Il explique notamment les fondements et les automatismes à la base de la détermination d'un socle de sécurité pour sécuriser, par conformité, au juste besoin, et en fonction des enjeux.

**Mots clefs[1]**

Sécurité des systèmes d'information, management des risques, besoins et enjeux de sécurité, démarche systématique, automatisation, socle de sécurité, référentiels de mesures, conformité

***A critical review of approaches to securing proportionally to the needs and stakes – with automation considerations***

*For a long time, there have been two main approaches to securing a system or organisation. On the one hand, compliance with respect to generic security baselines, and on the other, risk scenarios studies. However, these approaches have shown their limits: compliance is simple but rarely relates to the needs and stakes, whilst the risk scenario approach is exhaustive and specialised, but work intensive to propose many basic security controls. Thus, hybrid approaches have appeared. These hybrid approaches recommend first a step of securing by compliance, more or less ad hoc, conducive to a certain automation, then a step of scenario analysis, manual and based on expert judgement. These hybrid approaches reshuffle the cards from a societal and work organisation point of view, involving more the system engineers and architects, and free time for the cybersecurity experts, who can concentrate on difficult issues. However, the first step remains an operation that is still poorly controlled. This paper performs a critical review of the current norms and standards that propose this hybrid approach. It*

C&ESAR'21: Computer Electronics Security Application Rendezvous, November 16-17, 2021, Rennes, France
EMAIL: stephane.paul@thalesgroup.com (A.1); nicolas.vancauter@thalesgroup.com (A.2); paul.varela@thalesgroup.com (A.3); simon-mickael.leboeuf@thalesgroup.com (A.4); michael.catroux@thalesgroup.com (A.5)
ORCID: 0000-0003-2123-5370 (A.1), 0000-0001-9953-5360 (A.3)

*explains the fundamentals and the mechanisms underlying the determination of a security baseline to secure, by compliance, in line with the needs and stakes, which can be automated.*

## 1. Introduction

On a pu autrefois considérer la sécurisation des systèmes comme une combinaison coûts / délais qui pénalise la mise sur le marché ou la mise en service opérationnel. Un discours plus moderne intègre la sécurisation des systèmes dans une démarche qualité. On parle alors de système de management et d'amélioration continue de la sécurité, en posant en filigrane la question du coût de l'insécurité.

Les approches pour sécuriser un système (ou une organisation) se sont longtemps organisées en deux camps. Le premier camp privilégiait une approche par conformité vis-à-vis de référentiels de mesures de sécurité. Le représentant le plus emblématique de ces référentiels est le recueil de bonnes pratiques pour le management de la sécurité de l'information [1] du département du commerce et de l'industrie du gouvernement anglais de 1992, devenu successivement le BS 7799 en 1995, puis l'ISO/CEI 17799 en 2000, et enfin l'ISO/CEI 27002 [2] en 2007. A l'opposé, le second camp privilégiait une étude exhaustive de scénarios de risque, potentiels ou avérés, en tant qu'outil support à la prise de toute décision de sécurisation. Les représentants de cette approche incluent l'ISO/CEI 27005 [3], le NIST SP 800-30 [4], MEHARI [5], MAGERIT [6] ou les évolutions de la méthode EBIOS [7] jusqu'à la version EBIOS-2010 incluse.

Ces deux approches ont montré leurs limites. Selon une estimation du BSI [8], l'étude par conformité traite efficacement au mieux 80% des menaces, notamment celles qui sont de niveau faible à moyen. De plus, les mesures issues de cette approche ne sont pas toujours finement adaptées au besoin : elles peuvent être insuffisantes ou excessives. A contrario, l'étude exhaustive par scénarios de risques permet une couverture au plus juste, avec des mesures de sécurité ad hoc, mais elle est très couteuse.

Suite à ce constat, ces deux approches ont actuellement tendance à fusionner pour donner des démarches hybrides, avec la promesse du meilleur des deux mondes : d'abord une sécurisation par conformité vis-à-vis d'un socle de mesures de sécurité relativement ajusté aux besoins et enjeux de sécurité, puis une étape par scénarios de risque pour compléter ce socle, si et seulement si cela s'avère nécessaire.

Ces nouvelles démarches hybrides rebattent les cartes d'un point de vue sociétal et d'organisation du travail. En effet l'approche par scénarios a historiquement cantonné la sécurisation des systèmes aux mains des seuls spécialistes en sécurité de l'information, entrainant de fait une faible implication des métiers. A l'opposé, l'approche par conformité permettait sans doute trop facilement aux métiers de ne pas faire appel à ces mêmes spécialistes. Les démarches hybrides ouvrent la voie à un réel rééquilibrage : les ingénieurs et architectes généralistes prennent l'initiative sur certaines activités d'ingénierie de la cyber-sécurité. Ils libèrent ainsi du temps pour les experts, qui peuvent se concentrer sur des activités à haute valeur ajoutée.

Cependant, pour les ingénieurs et architectes généralistes qui font leurs premiers pas en cybersécurité, mais aussi pour les spécialistes habitués à procéder uniquement par scénarios de risque, ce premier niveau de sécurisation avec un socle de sécurité reste une opération globalement mal maîtrisée qu'une automatisation pourrait simplifier.

Nous avons introduit la notion de socle de sécurité. Il s'agit d'un ensemble d'exigences de sécurité, issues de textes réglementaires, de normes et standards (notamment les guides d'hygiène), d'obligations contractuelles, et/ou de la politique de sécurité des systèmes d'information interne à l'organisation. La définition de ces socles de sécurité peut être systématisée, voire automatisée. Pour un système, une ligne de produits ou une organisation, la définition d'un socle de sécurité permet d'imposer un ensemble de mesures de sécurité sans qu'il ne soit nécessaire de justifier chaque mesure par l'identification des risques. La justification est apportée indépendamment de l'étude par l'historique des atteintes passées et/ou par le niveau de maturité que l'organisation cherche à atteindre et/ou par un lien préalablement établi entre ces mesures de sécurité et les menaces qui pèsent sur le sujet de l'étude.

Devant la montagne de référentiels de processus, de patrons d'architecture et/ou de mesures de sécurité disponibles, il n'est pas toujours facile de faire un choix éclairé, de distinguer le nécessaire du superflu. Juste pour

citer quelques exemples, il existe des standards de cybersécurité :

- Génériques, e.g., les familles ISO/CEI 27k [9], NIST SP 800 [10], les mesures minimum de sécurité de l'ENISA [11] issues des travaux de la directive européenne 2016/1148 [12] (usuellement désignée sous les noms de *Directive SRI*) ou encore, l'IT-Grundschutz Kompendium [13],
- Par profil technique, e.g., ISA/CEI 62443 [14] pour les systèmes de contrôle industriels, ou SecNumCloud [15] pour l'informatique en nuage,
- Par domaine d'activité, e.g., l'ISO/CEI 80001 [16] pour les équipements médicaux, l'ISO/SAE DIS 21434 [17] pour l'information automobile, ou PCI [18] pour la protection des données de comptes.

Par ailleurs, les démarches hybrides les plus matures ne font pas que juxtaposer une approche par conformité et une approche par scénario. La détermination du socle de sécurité devient une activité d'ingénierie à part entière, afin que ce dernier soit le plus adapté possible aux besoins et enjeux de sécurité du contexte étudié. Un socle bien ajusté réduit l'étude par scénario de risque au minimum. Typiquement, il n'est plus question d'appliquer toutes les mesures d'un référentiel (e.g., l'ISO/CEI 27002 [2]) sans réfléchir au préalable à l'adéquation entre ces mesures et les besoins et enjeux.

Cette publication analyse comment les nouvelles démarches hybrides aident à sécuriser un système par conformité au juste besoin et/ou de façon proportionnée aux enjeux. Elle commence par définir ce qu'est le juste besoin et la notion d'enjeu (cf. chapitre 2). La maîtrise préalable de ces notions est un prérequis à l'automatisation de l'identification du socle de sécurité. Elle dresse ensuite un panorama de plusieurs démarches hybrides, en détaillant comment chacune propose de déterminer le socle de sécurité (chapitre 3) ; l'automatisation de cette détermination est discutée. Enfin, une synthèse met en avant les forces et faiblesses des différentes méthodes (cf. chapitre 4). Ce papier n'aborde pas le volet de sécurisation par scénario des différentes méthodes car, étant actuellement avant tout à dire d'experts, il ne se prête pas trivialement à une automatisation.

## 2. Besoins et enjeux de sécurité

Lorsqu'on réalise une étude de sûreté de fonctionnement dans le monde de l'avionique, une donnée d'entrée importante est le niveau cible de sûreté de fonctionnement à tenir, généralement exprimé en nombre d'accidents par heure de vol, typiquement $10^{-7}$. L'étude consistera alors à s'assurer que cette cible est atteinte, éventuellement avec une petite marge.

Lorsque l'on réalise une étude de cybersécurité, il n'y a personne pour nous fixer une telle cible. Viser trop bas expose l'organisation à des conséquences qu'elle ne pourra peut-être pas assumer. Viser trop haut engendre des coûts injustifiables. Alors, comment déterminer le juste besoin[2] de sécurité ? et comment s'assurer d'une sécurisation proportionnée aux enjeux ?

### 2.1. Identifier les besoins

Le besoin de sécurité est intrinsèquement lié au domaine d'activité. On sent confusément que la détermination du besoin n'est pas du ressort du seul spécialiste en cybersécurité. Ce dernier doit solliciter le support de la direction pour comprendre la politique / stratégie de l'organisation et des experts métier pour comprendre les raisons qui sous-tendent les besoins exprimés. L'objectif est de déterminer avec eux le seuil de perturbations à partir duquel le système n'est plus considéré en fonctionnement nominal.

De façon générale, les besoins de sécurité s'expriment en termes de critères de disponibilité, d'intégrité et de confidentialité (D-I-C) vis-à-vis de leurs valeurs métier. Certaines communautés peuvent y rajouter d'autres critères, comme par exemple l'authenticité dans la directive SRI [12].

La première étape pour l'identification du besoin consiste à sélectionner, avec les experts métier, les critères de sécurité pertinents. Chacun de ces critères s'exprime avec une échelle. La définition de l'échelle dépend du domaine, voire de l'organisation, ou du système étudié dans son contexte d'emploi. Pour une activité de contrôle aérien, l'échelle pour le critère de disponibilité s'exprimera vraisemblablement en millisecondes d'indisponibilité. Par contraste, pour un travail administratif /

[2] Dans ce contexte, deux notions sont couramment utilisées, parfois à tort : celle de *besoin de sécurité* et celle d'*objectif de sécurité*. Nous utiliserons ici les définitions de l'ISO/CEI 27003 [17].

bureautique, l'échelle s'exprimera probablement en nombre d'heures d'indisponibilité.

Toujours avec les experts métier, la seconde étape pour l'identification du besoin consiste à fixer, pour chaque critère de sécurité, les différents niveaux au sein de cette échelle. Il faut ici se poser la question du sens de chaque échelon. Par exemple, y-a-t-il une vraie différence opérationnelle entre un temps de réponse du système de 50 ms et un temps de réponse de 200 ms ? Si oui, alors un palier peut effectivement être défini.

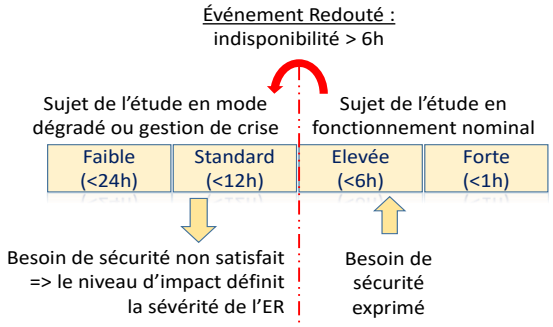


Figure 1 : Définition du besoin en disponibilité

Supposons par exemple une échelle pour le critère de disponibilité (cf. Figure 1), avec quatre niveaux (Faible, Standard, Elevée, Forte) définissant la durée d'indisponibilité maximale autorisée pour une valeur métier (respectivement 24h, 12h, 6h et 1h).

La troisième et dernière étape pour l'identification du besoin consiste à déterminer le seuil à partir duquel le sujet de l'étude quitte son fonctionnement nominal, et rentre en gestion de crise. Ce seuil est une ligne rouge que la valeur métier ne doit pas franchir (cf. Figure 1). Sur l'échelle du critère de sécurité, le dernier niveau acceptable avant le franchissement de ce seuil est défini comme étant le besoin de sécurité pour ce critère. Le franchissement de ce seuil s'appelle un événement redouté. Dans l'exemple de la Figure 1, le besoin est exprimé pour une disponibilité *Elevée*, et l'événement redouté correspond à une indisponibilité de la valeur métier allant au-delà des six heures.

Le besoin de sécurité étant maintenant identifié, il convient de déterminer la gravité du franchissement de la ligne rouge.

## 2.2. Identifier les enjeux

En correspondance du besoin de sécurité, et de l'évènement redouté qui en découle, est associé une gravité. La gravité est une mesure des enjeux liés à la non-tenue du besoin. Comme les besoins de sécurité, la gravité s'exprime au moyen d'une échelle. Voici quelques exemples :

- Le guide de la méthode EBIOS - Risk Manager [19] définit une échelle de 4 niveaux : G1 – mineure, G2 – significative, G3 – grave, et G4 – critique ;
- Le NIST FIPS 199 [20] définit une échelle à 3 niveaux de gravité : *Low* (faible), *Moderate* (modérée) et *High* (élevée) ;
- La société Thales définit, dans les guides de cybersécurité [21] [22] pour ses propres architectes système, une échelle à 5 niveaux, numérotée de 1 à 5.

Dans la mesure où un événement redouté traduit une sortie du mode nominal, il est possible de lister les conséquences négatives de la survenue de cet événement, et d'accoler à chaque conséquence un niveau d'impact.

Le niveau d'impact s'exprime lui aussi au moyen d'une échelle. Là encore, la liste des conséquences, avec leurs types et leurs niveaux d'impact, peut être définie spécifiquement pour l'étude, reprise d'un guide méthodologique, d'une norme ou d'un standard ou mieux encore, du référentiel de l'organisation. Typiquement, le standard anglais HMG Information Assurance Standard No.1 [23] définit plusieurs échelles de niveaux d'impact pour différents secteurs d'activité, dont la défense, les relations internationales, le commerce, les infrastructures critiques, ou encore la vie et la santé des personnes (cf. **Table 1**).

La définition des échelles de gravité et de niveaux d'impact doit s'accompagner d'une mise en relation entre les niveaux d'impacts et les niveaux de gravité. Par exemple, si l'on retient l'échelle de gravité du guide de la méthode EBIOS - Risk Manager [19] et l'échelle d'impacts du standard anglais HMG Information Assurance Standard No.1 [23], on pourrait choisir de dire que :

- Les niveaux d'impact 0 à 2 correspondent à une gravité G1 – mineure ;
- Le niveau d'impact 3 correspondent à une gravité G2 – significative ;
- Le niveau d'impact 4 correspondent à une gravité G3 – grave ;
- Les niveaux d'impact 5 à 6 correspondent à une gravité G4 – critique.

**Table 1**
Extrait et traduction du standard anglais HMG Information Assurance Standard No.1

| Catégorie | Niv. 0 | Niv. 1 | Niv. 2 | Niv. 3 | Niv. 4 | Niv. 5 | Niv. 6 |
|---|---|---|---|---|---|---|---|
| **Vie et santé des gens** | | | Inconfort d'un individu | Atteinte à la sécurité ou la liberté d'un individu | Atteinte à la sécurité ou la liberté d'un groupe de personnes | Atteinte à la vie d'un groupe de personnes | Perte massive de vies humaines |

Une fois établi la corrélation entre niveaux d'impacts et niveaux de gravité, il suffit de lister les conséquences d'un événement redouté pour en déduire la gravité. De plus, cette corrélation peut être réutilisée à travers plusieurs études. Elle assure une automatisation[3] de l'identification de la gravité, ainsi qu'une cohérence des appréciations à travers les différents intervenants sur une étude. En effet, le travail sur les seules conséquences est souvent plus objectif que le choix d'un niveau de gravité ex nihilo.

## 2.3. Besoins versus enjeux

Dans notre démarche jusqu'ici, nous avons montré comment identifier un besoin de sécurité, puis comment estimer l'enjeu du non-respect de ce besoin au moyen de la gravité de l'événement redouté associé. A ce stade, il est fréquent de faire un amalgame entre niveau du besoin de sécurité et gravité du non-respect de ce besoin. Il est en effet assez intuitif de penser que plus le besoin serait fort, et plus la gravité de sa violation serait forte. Ceci n'est pourtant pas toujours vrai. Pour les trois critères (i.e. disponibilité, intégrité et confidentialité), nous allons présentement montrer qu'il est possible qu'un besoin soit exprimé en bas de l'échelle des besoins, mais que son non-respect soit critique, ou qu'inversement, un besoin soit exprimé en haut de l'échelle, mais que les conséquences de son non-respect soient mineures.

**Disponibilité**. Soit un système de communication radio de haute disponibilité pour une équipe d'intervention au sol. En cas de perte de la communication, la gravité ne serait que modérée, car une procédure consistant à envoyer une équipe de récupération sur la dernière position connue est une solution envisageable techniquement à un coût tolérable. A l'inverse, le niveau de disponibilité exprimé pour un système de contrôle d'une sonde spatiale peut être assez faible, alors même que le non-respect de ce besoin (c'est à dire une indisponibilité totale nécessitant une intervention manuelle de réparation) serait catastrophique, car synonyme de la perte définitive de la sonde.

**Intégrité**. L'illustration avec le critère d'intégrité est un peu plus délicate car les échelles d'intégrité sont moins intuitives. Définissons l'échelle suivante pour l'intégrité d'une information :

- I1 : la donnée peut être corrompue ;
- I2 : la donnée peut être corrompue, mais cet état de corruption est alors connu ;
- I3 : comme I2, mais un moyen est offert pour solliciter à nouveau la donnée jusqu'à ce qu'elle soit intègre ;
- I4 : la donnée est toujours intègre.

En s'appuyant sur cette échelle d'intégrité, il va être illustré que les conséquences du non-respect de l'intégrité d'une donnée classée I2 peuvent être plus graves que le non-respect de l'intégrité d'une donnée classée I4. Ainsi les informations de positions et de vitesses des avions données par un radar primaire à un contrôleur aérien sont classées I2. Une position corrompue mais signalée comme intègre par le système, et donc interprétée comme intègre par le contrôleur aérien, peut mener à un accident entre deux avions. Du point de vue d'un passager, cela peut signifier sa mort. A l'inverse, il est crédible d'imaginer que la consommation électrique d'un ménage français, calculé par le compteur Linky, est classée I4. Du point de vue d'un consommateur lambda, une erreur d'intégrité sur son compteur entrainera au plus une sur- ou une sous-facturation de quelques centaines d'euros.

**Confidentialité**. Soit une information classifiée au niveau Confidentiel – Union Européenne (C-UE) et une autre information classifiée au niveau Secret – Union Européenne (S-UE). Ces deux classifications relèvent du pénal, cependant le code pénal français (art. 411-7 et 413-10) retient comme critère discriminant, non pas le niveau de sensibilité de

[3] Si la méthode est outillée, il est souhaitable que la gravité calculée puisse éventuellement être remplacée manuellement par une valeur proche (plus forte ou plus faible), dans la mesure où cette modification est explicitement justifiée.

l'information compromise (i.e. son besoin de sécurité), mais le niveau d'intentionnalité de la compromission. Ainsi la peine encourue pour une compromission intentionnelle d'une information p. ex. C-UE est plus lourde (10 ans d'emprisonnement et 150 000€ d'amende) que pour la compromission par négligence d'une information p. ex. S-UE (3 ans d'emprisonnement et 45 000€ d'amende).

Nous venons de montrer que les niveaux du besoin de sécurité et de gravité de l'évènement redouté associé (c'est à dire l'enjeu) ne représentent pas la même chose. Ce sont deux dimensions complémentaires utiles pour la détermination des mesures de sécurité. Le niveau des besoins de sécurité détermine le « niveau de force » à mettre dans les mesures de sécurité, tandis que les enjeux déterminent le « niveau de garantie » sur l'efficience de ces mesures.

Ces deux leviers fonctionnent selon des logiques différentes. Le besoin de sécurité exprime le *coût à faire* de la sécurité. Plus le niveau du besoin de sécurité est élevé, plus les mesures de sécurité devront être fortes, et donc généralement coûteuses. Par contraste, la gravité de l'évènement redouté exprime le *coût à ne pas faire* suffisamment de sécurité pour empêcher l'événement redouté de survenir. Il ne s'agit pas là de mettre en place des fonctions de sécurité plus fortes, mais de s'assurer de la bonne mise en œuvre, de la résistance et/ou de la résilience des mesures précitées. Cela se traduit généralement par des mesures de vérification et validation. Une bonne maîtrise de la distinction entre ces deux notions est primordiale pour l'automatisation du choix du socle de sécurité. Le niveau du besoin de sécurité guidera la sélection des mesures de sécurité fonctionnelles, et le niveau des enjeux guidera le choix des mesures de sécurité non-fonctionnelles complémentaires pour obtenir le niveau de garantie requis sur l'efficience des mesures de sécurité fonctionnelles.

**Exemple**. Soient deux informations que l'on veut intègres durant tout leur cycle de vie (i.e. niveau I4 dans l'échelle donnée ci-dessus). D'un côté la trace d'un système d'enchères en ligne entre particuliers ; la trace doit servir de preuve en cas de contestation. De l'autre côté, les coordonnées d'une cible affectée à un missile. Dans les deux cas, le besoin d'intégrité implique l'usage d'une fonction de hachage cryptographique. Cependant, il existe un grand nombre d'algorithmes de hachage, plus ou moins résistants aux attaques, sans compter la qualité de l'implémentation de ces algorithmes. Dans le cas du système d'enchères, le niveau d'impact d'une altération de la trace serait vraisemblablement modéré : impact financier, impact d'image. Dans le cas du système de tir, le niveau d'impact d'une altération des coordonnées serait vraisemblablement critique : impact sur la vie humaine, impact juridique, impact géopolitique. De ces différentes gravités, on peut justifier les deux décisions suivantes. Pour le site d'enchères, une fonction de hachage de type MD5 issue d'une bibliothèque standard en source ouverte. Pour le système de missiles, une fonction de hachage de type SHA-2 issue d'une bibliothèque de fonctions cryptographiques ayant fait l'objet d'une preuve formelle de niveau EAL7. Ces deux décisions, qu'on pourrait qualifier ici de raisonnables, résultent en fait de l'aversion au risque du décisionnaire. Elles sont automatisables sous condition d'une très bonne maîtrise des notions de besoin et d'enjeu de sécurité.

## 2.4. Conclusion partielle

Nous avons rappelé (cf. chapitre 1) que les nouvelles démarches de sécurisation hybrides procèdent en deux étapes : d'abord une sécurisation par conformité vis-à-vis d'un socle de mesures de sécurité plus ou moins ad-hoc, puis une étape par scénarios de risque pour compléter ce socle, si nécessaire.

Nous avons ensuite montré (cf. chapitre 2) comment le besoin de sécurité et la gravité du non-respect de ce besoin sont deux notions complémentaires qui doivent être utilisées de concert pour déterminer les mesures de sécurité fonctionnelles et non-fonctionnelles les mieux ajustées aux besoins et aux enjeux de sécurité.

Nous allons maintenant voir (cf. chapitre 3) que ce type de raisonnement sur les besoins et les enjeux, auquel il faut ajouter la prise en compte du niveau des cyberattaques, est à la base de la détermination des socles de sécurité de la plupart des nouvelles démarches hybrides. En effet, alors que les approches par conformité ont tendance à appliquer sans état d'âme un catalogue entier de mesures de sécurité (e.g. l'ISO 27001 et son catalogue ISO 27002), les démarches hybrides tendent à sélectionner, plus ou moins finement, les mesures à insérer dans le socle. Cette sélection fine se fait sans réaliser

d'analyse de risque à proprement parler, notamment sans analyse de vulnérabilités.

Ce qui est particulièrement intéressant, c'est que la démarche de détermination du socle peut être systématisée, et mise à la portée de tous, y compris des non-spécialistes en cybersécurité.

Nous allons maintenant effectuer un état de l'art des principales démarches hybrides qui instancient toutes plus ou moins ce cheminement. Nous discuterons ensuite de l'automatisation possible de ces démarches.

## 3. Les grandes démarches hybrides

Toutes les démarches de management des risques présentées ci-dessous préconisent une sélection d'un socle de sécurité en préalable à une évaluation des risques de sécurité à base de scénarios. Leur choix a été motivé par le fait qu'il existe d'importantes disparités entre elles sur la façon de déterminer ce socle, avec des compromis sur la simplicité de la démarche, et la généricité du résultat, notamment sur le niveau d'ajustement du socle aux besoins et aux enjeux.

Cet état de l'art ne s'intéresse qu'à la partie méthodologique concernant la sélection d'un socle de sécurité et sa potentielle automatisation. Elle ne présente pas la démarche globale de management des risques.

### 3.1. EBIOS - Risk Manager

La sécurisation par conformité est une des nouveautés de la méthode EBIOS - Risk Manager [19] par rapport à l'ancienne version de la méthode, dite EBIOS-2010. Avec EBIOS - Risk Manager, le socle est déterminé selon la pyramide du management du risque numérique (cf. Figure 2). Par postulat, une bonne hygiène informatique générique [24] permet de lutter efficacement contre les attaques *simples*. Pour des cyberattaques de niveau *élaboré*, le socle doit s'enrichir des normes et textes règlementaires applicables. Selon l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), le socle de sécurité est donc donné pour un niveau donné de cyber-attaques, en l'occurrence de *simple* à *élaboré*. On retrouve ici en filigrane le résultat de l'étude du BSI [8] indiquant que le socle de sécurité permettrait de traiter 80% des attaques.

Selon la méthode, l'appréciation des risques par scénarios n'est réalisée que pour les systèmes ou organisations faisant face aux attaques les plus avancées et dont le socle de sécurité aura été préalablement implémenté. Il est à noter que la méthode fait l'hypothèse que les risques accidentels et environnementaux sont entièrement traités par le socle de sécurité. De ce fait, l'appréciation des risques par scénarios ne s'intéresse qu'aux seuls risques numériques intentionnels.

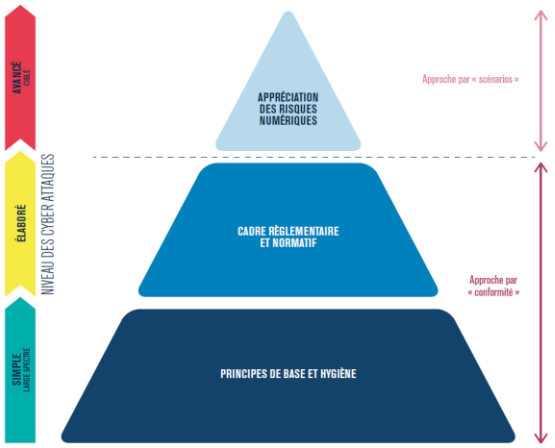


Figure 2 : Pyramide du management du risque

Concernant les règles d'hygiène, l'ANSSI propose un catalogue de 42 mesures [24]. Ce catalogue est structuré en règles de niveau *standard* ou de niveau *avancé*.

En complément, pour aussi couvrir les attaques élaborées, l'ANSSI a publié ces dernières années un certain nombre de guides de bonnes pratiques sur des thématiques précises, avec en fil rouge une approche par niveaux de mise en œuvre, dite MIRE (pour Minimal, Intermédiaire, Renforcé, Elevé), qui facilite l'extraction automatique des règles. Pour le cadre réglementaire, la méthode renvoie vers une page web [25]. Cependant les textes qui s'y trouvent n'ont pas été rédigés en ayant à l'esprit leur utilisation pour construire un socle de sécurité. En attendant leur mise à jour, leur traitement automatisé n'est pas aisé.

Pour finir, il est à regretter que la méthode n'explique ni comment doit se faire la sélection des référentiels, ni le niveau de granularité ou de profondeur attendu. Les règles des guides de bonnes pratiques, avec leur niveau MIRE associé, peuvent cependant être un bon point de départ. L'utilisation de ces niveaux permet l'établissement de groupes de mesures de sécurité à appliquer de manière automatique dans des exigences projets en fonction du besoin de sécurité exprimé.

## 3.2. NIST

Le cadre de management du risque du NIST SP 800-37 [26] définit deux approches pour sélectionner un socle de sécurité : soit par la sélection d'un profil générique, soit par la sélection d'un profil ad-hoc.

Le NIST SP 800-53B [27] est un bon exemple de profil relativement générique. Ce standard s'applique à toutes les informations et tous les systèmes du gouvernement fédéral américain (cf. Figure 3**)**. Les standards NIST SP800-171 [28] et NIST SP800-172 [29] sont de bons exemples de profils ad-hoc. Ces derniers s'appliquent uniquement à la confidentialité des informations *contrôlées non classifiées* du gouvernement fédéral lorsqu'elles sont manipulées par un système non fédéral.

Les mesures incluses dans les profils du NIST SP 800-53B sont celles des catalogues NIST SP 800-53 [30] et NIST SP 800-53A [31]. Ces catalogues listent un ensemble de près d'un millier de mesures de sécurité, respectivement fonctionnelles et non-fonctionnelles, réparties en vingt familles. Pour les informations et systèmes du gouvernement fédéral américain, les profils du NIST SP 800-53B sont sélectionnés exclusivement en fonction de la gravité des enjeux. L'échelle de gravité à utiliser est définie par le NIST FIPS-199 [20].

Ce standard définit, pour chacun des trois critères D-I-C, trois niveaux possibles de gravité : *Low* (faible), *Mod* (modéré) et *High* (élevé).

Un préalable à l'utilisation du NIST SP 800-53B est la catégorisation du système. Cette catégorisation consiste à définir un niveau d'enjeu unique pour tout le système.

Selon le NIST FIPS 200 [32], ce niveau d'enjeu unique, transverse aux différents critères de sécurité, est défini comme étant égal à la plus forte des gravités de tous les événements redoutés.

La Figure 3 illustre un extrait du NIST SP 800-53B focalisé sur la famille des mesures de contrôle d'accès. Elle montre notamment que, quels que soient les enjeux, la définition de la politique et des procédures de contrôle d'accès (AC-1), ainsi qu'une gestion des comptes (AC-2) sont nécessaires. En revanche, l'automatisation de cette gestion des comptes (AC-2(1)) n'est requise que lorsque la gravité des enjeux est *Mod* (modéré) ou *High* (élevé).

Les standards NIST SP 800-171 et NIST SP 800-172 s'appuient eux aussi sur les catalogues NIST SP 800-53 et NIST SP 800-53A, mais la sélection des socles n'est plus basée exclusivement sur la gravité des enjeux.

| CONTROL NUMBER | CONTROL NAME<br>CONTROL ENHANCEMENT NAME | PRIVACY CONTROL BASELINE | SECURITY CONTROL BASELINES | | |
|---|---|---|---|---|---|
| | | | LOW | MOD | HIGH |
| **AC-1** | **Policy and Procedures** | x | x | x | x |
| **AC-2** | **Account Management** | | x | x | x |
| AC-2(1) | AUTOMATED SYSTEM ACCOUNT MANAGEMENT | | | x | x |
| AC-2(2) | AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT | | | x | x |
| AC-2(3) | DISABLE ACCOUNTS | | | x | x |

Figure 3 : Famille de mesures de contrôle d'accès du NIST SP 800-53B

| ID | TITLE | Confidentiality | | | Integrity | | | Availability | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | L | M | H | L | M | H | L | M | H |
| AC-1 | Access Control Policy and Procedures | X | X | X | X | X | X | X | X | X |
| AC-2 | Account Management | X | X | X | X | X | X | | | |
| AC-2(1) | Account Management \| Automated System Account Management | | X | X | | X | X | | | |
| AC-2(2) | Account Management \| Removal of Temporary / Emergency Accounts | | X | X | | X | X | | | |

Figure 4 : Famille de mesures de contrôle d'accès du CNSS 1253

La sélection s'appuie aussi sur le besoin de sécurité (en l'occurrence ici, la confidentialité des informations *contrôlées non classifiées*), et le niveau des cyberattaques. Notamment, le NIST SP 800-171 définit un profil correspondant à un sous-ensemble du profil *Mod* (modéré) du NIST SP 800-53B, en ne retenant que les exigences pertinentes vis-à-vis de la confidentialité. Les exigences du NIST SP 800-172 complètent celles du NIST SP 800-171 pour lutter plus efficacement contre des menaces persistantes avancées (APT). De fait, les standards NIST SP 800-171 et NIST SP800-172 peuvent aussi être vus comme les réponses à un même niveau de besoin de sécurité face à deux niveaux différents de cyberattaque.

Les standards proposés par le NIST sont les plus avancés en matière d'automatisation. Leur utilisation importante, notamment sur le marché américain, permet à la communauté scientifique de bénéficier de ces bases sous différents formats (Excel, OSCAL, etc.) permettant de les intégrer facilement dans des outils de gestion d'exigences et de conformité, ou bien dans des outils de déploiement automatique de mesures de sécurité, comme cela sera expliqué par la suite dans cette publication.

## 3.3. NSA

La démarche de la NSA est une amélioration de la méthode du NIST. Elle est basée sur le même jeu de documents, sauf que le NIST SP 800-53B [27] est remplacé par le CNSS 1253 [33]. Le CNSS 1253 propose lui aussi un découpage des mesures du NIST SP 800-53 en trois profils correspondant à la gravité des enjeux de sécurité, cependant il le fait cette fois pour chacun des trois critères de sécurité (disponibilité, intégrité et confidentialité) indépendamment.

La Figure 4 illustre un extrait du CNSS 1253 focalisé sur les mesures de contrôle d'accès. Elle montre que, quels que soient les enjeux, la définition de la politique et des procédures de contrôle d'accès est toujours nécessaire. En revanche, une gestion des comptes n'est nécessaire que pour assurer la confidentialité et l'intégrité du système.

L'approche de la NSA comble ainsi le défaut majeur de l'approche du NIST, notamment pour les systèmes civils et commerciaux. Par exemple, sur un système de contrôle de trafic aérien, une violation des besoins de disponibilité ou d'intégrité peut conduire à un accident d'avion, et la perte de centaines de vies humaines. Selon le NIST, le système serait donc catégorisé selon le profil de gravité *High* (élevée), ce qui impliquerait un niveau élevé aussi pour les exigences en confidentialité, et donc le chiffrement de toutes les communications sol-bord. Ceci ne serait pas une solution commercialement acceptable. La démarche de la NSA est donc extrêmement efficace dans la recherche d'une sécurisation qui soit à la fois au juste besoin et en adéquation aux enjeux.

## 3.4. BSI IT-Grundschutz

L'approche du BSI pour la détermination du socle de sécurité s'appuie sur deux documents : le BSI-Standard 200-2 [34], qui définit la méthode, et le référentiel IT-Grundschutz-Kompendium [13].

La méthode introduit trois profils de protection nommés *Basic* (de base), *Core* (fondamental) et *Standard*. Une des originalités de l'approche du BSI est que ces profils comprennent à la fois un processus de sécurisation et un socle de mesures de sécurité adaptés à la problématique. Le profil de protection *Basic* offre un processus de sécurisation simple et une hygiène de base pour les petites entreprises ou celles à faible maturité en cybersécurité. Le profil de protection *Core* vise uniquement le sous-ensemble fondamental des processus et des ressources d'une organisation, les fameux joyaux de la couronne. Le profil de protection *Standard* offre un niveau de sécurité uniformément haut. Il représente l'approche classique de l'IT-Grundschutz, et est celui qui développe le plus loin l'utilisation du socle de mesures de sécurité. Notamment, il permet d'affiner le choix des exigences en fonction des enjeux (c'est à dire la gravité des conséquences du non-respect des besoins de sécurité). Le BSI-Standard 200-2 [34] définit trois niveaux d'enjeux : Normal, Haut, et Très Haut. Ces niveaux n'influencent cependant qu'à la marge le choix des exigences.

Une particularité du catalogue de l'IT-Grundschutz est de mettre en relation des menaces élémentaires et les exigences qui contribuent à leur couverture. Cette matrice (cf. Figure 5) peut être vue comme le lien entre le référentiel de sécurité et le résultat d'une analyse de risque exhaustive par scénario basée sur l'étude des menaces élémentaires. Elle

permet notamment de faire le lien entre une non-conformité par rapport au socle de sécurité et les analyses par scenarios : une non-conformité sur une mesure de sécurité permet de manière automatique d'identifier la ou les menaces élémentaires à intégrer dans les scenarios de risque. La réciproque est également vraie : l'utilisation de cette matrice permet de venir enrichir le socle de sécurité de manière automatique suite à l'identification de menaces élémentaires utilisées pour la définition de scenarios de risques critiques pour l'organisation. Cette approche structurée et systématique participe à donner des capacités d'automatisation du socle de sécurité. Le BSI se sert de cette approche pour justifier de l'inutilité d'une analyse de risque par scénarios à part entière pour les systèmes d'information (SI) courants, et cela sans remettre en cause la qualification à une certification ISO/CEI 27001 [35]. En revanche, pour les SI le nécessitant, le BSI propose bien une méthode d'analyse par scénario (cf. BSI-Standard 200-3 [36]) pour compléter le socle de sécurité de manière ad hoc.

| Elementary Threats / Requirements | G 0.14 | G 0.16 | G 0.17 | G 0.18 | G 0.19 | G 0.22 | G 0.25 | G 0.26 | G 0.27 | G 0.29 | G 0.38 | G 0.45 | G 0.46 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ORP.1.A1 | X | | | X | X | X | | | | X | X | | X |
| ORP.1.A2 | X | X | | X | X | X | X | X | X | X | X | | X |
| ORP.1.A3 | X | X | | | X | X | | | | | | | |
| ORP.1.A4 | | | | | X | X | | | | X | X | | |
| ORP.1.A5 | X | X | | | X | X | | | | | X | | X |

Figure 5 : Exemple de mise en relation de menaces et d'exigences de sécurité (BSI)

Une autre particularité du catalogue de l'IT-Grundschutz est son niveau de détail. La plupart des catalogues standardisés sont neutres au niveau politique, et neutres au niveau technologique. Ce n'est pas le cas du catalogue de l'IT-Grundschutz, qui aborde par exemple les différentes versions du système d'exploitation Windows, et bien d'autres technologies, e.g. l'internet des objets, l'informatique dans les nuages, la 5G, etc.

Pour éviter l'obsolescence de son catalogue, le BSI le met à jour annuellement, du moins dans sa version officielle, qui est en allemand. Une traduction en anglais en est assez souvent proposée, sur la base du *final draft* de la version allemande, donc sans support officiel par le BSI.

## 3.5. ISA/CEI 62443

L'ISA/CEI 62443 [14] définit cinq niveaux de sécurité qui traduisent la résistance d'un système de contrôle industriel à différentes classes d'attaquants :

- *SL 0*: aucune exigence ou protection particulière n'est requise.
- *SL 1*: protection contre les abus involontaires ou accidentels.
- *SL 2*: protection contre les abus intentionnels par des moyens simples avec peu de ressources, des compétences générales et une faible motivation.
- *SL 3*: protection contre une utilisation abusive intentionnelle, par des moyens sophistiqués, avec des ressources modérées, des connaissances spécifiques, et une motivation modérée.
- *SL 4*: protection contre les utilisations abusives intentionnelles, à l'aide de moyens sophistiqués, dotés de ressources étendues, de connaissances spécifiques et d'une forte motivation.

Une fois le niveau de protection choisi, il suffit de sélectionner les mesures correspondantes au sein du catalogue. Cette sélection peut donc être réalisée de manière automatique.

La Figure 6 illustre un extrait de l'ISA/CEI 62443-3-3 [37] concernant la famille des mesures d'identification et d'authentification. On peut y voir qu'un système d'identification et d'authentification est requis quel que soit le niveau de sécurité, mais qu'une authentification unique n'est requise qu'à partir du niveau *SL 2*, et qu'une authentification multi-facteurs n'est requise qu'à partir des niveaux *SL 3* ou *SL 4*, selon que le réseau soit ou non de confiance.

L'ISA/CEI 62443 organise ses mesures de sécurité en sept familles. Une des particularités de l'approche est que le niveau de sécurité peut être variable d'une famille à l'autre. On parle alors de vecteur de niveaux de sécurité. Par contre, au sein d'une famille donnée, toutes les mesures d'un niveau doivent être sélectionnées pour valider le niveau.

Par ailleurs, pour éviter d'imposer un même jeu de mesures, éventuellement très contraignant, à tout le système, l'ISA/CEI 62443 prévoit un découpage du système en zones et conduits. La détermination du socle se fait alors par zone, en fonction du niveau de sécurité requis pour chaque zone.

| SRs and REs | | SL 1 | SL 2 | SL 3 | SL 4 |
|---|---|---|---|---|---|
| **FR 1 – Identification and authentication control (IAC)** | | | | | |
| SR 1.1 – Human user identification and authentication | 5.3 | ✓ | ✓ | ✓ | ✓ |
| SR 1.1 RE 1 – Unique identification and authentication | 5.3.3.1 | | ✓ | ✓ | ✓ |
| SR 1.1 RE 2 – Multifactor authentication for untrusted networks | 5.3.3.2 | | | ✓ | ✓ |
| SR 1.1 RE 3 – Multifactor authentication for all networks | 5.3.3.3 | | | | ✓ |
| SR 1.2 – Software process and device identification and authentication | 5.4 | | ✓ | ✓ | ✓ |
| SR 1.2 RE 1 – Unique identification and authentication | 5.4.3.1 | | | ✓ | ✓ |

Figure 6 : Extrait de l'ISA/CEI 62443-3-3

La combinaison des vecteurs de niveaux et du découpage en zones et conduits permet un ajustement très fin du socle de sécurité aux besoins de sécurité. Notons pour finir que ce standard ne rend obligatoire l'analyse de risque après la détermination du socle que s'il y a des écarts dans l'application du socle.

## 3.6. Thales

Historiquement, Thales a défini des méthodes et référentiels de sécurité différents pour répondre à ses besoins internes et aux besoins de ses clients. Nous présentons brièvement ici deux de ces approches :

- l'approche de la direction de la sécurité des systèmes d'information (SSI) pour les besoins propres aux SI internes de Thales, et qui s'appuie sur une base EBIOS;
- l'approche du référentiel d'ingénierie du Groupe Thales à l'usage des ingénieurs et architectes qui développent les systèmes que Thales vend à ses clients, et qui s'appuie sur une base NIST.

Pour la sécurisation de ses SI internes, Thales a défini son propre référentiel, qui comprend un peu plus de 350 exigences de sécurité. La sélection d'un socle de sécurité dans ce référentiel pour un SI donné s'effectue en fonction des besoins de sécurité exprimé pour ce SI selon les critères D-I-C.

Chaque critère de sécurité est défini par une échelle croissante à quatre niveaux, à savoir D1..D4, I1..I4, et C1..C4. Pour chaque exigence de sécurité du référentiel, un tableau indique les niveaux de besoin pour lesquels cette exigence doit être retenue.

Par exemple, sur l'extrait du référentiel de la Figure 7, on peut voir que l'authentification multi-facteur est nécessaire uniquement pour les SI manipulant des valeurs métiers dont le besoin en intégrité et en confidentialité est maximal, i.e. I4 et C4. Sur la ligne au-dessous, on peut constater par contre que la protection des informations d'authentification est systématiquement obligatoire, puisque nécessaire à partir d'un besoin d'intégrité minimal, i.e. I1.

La détermination et le traitement des socles de sécurité appellent de l'outillage et de l'automatisation. La SSI Thales s'appuie sur un outil de gestion des exigences qui est utilisé pour gérer la base de référence des exigences (i.e. le socle de sécurité). Cet outil permet notamment de générer à la demande des tableaux ou des documents structurés pré-remplis avec les éléments sélectionnés du socle, via des requêtes contenant les besoins D-I-C du système à sécuriser.

Pour les ingénieurs et architectes qui développent les systèmes que Thales vend à ses clients, Thales a défini d'autres référentiels de mesures de sécurité, ainsi qu'un processus de sélection de mesures proche de celui de la NSA (voir section 3.3). Une des grandes forces de cette approche est que les référentiels sont adaptés au domaine d'application. Typiquement, Thales a défini un guide dédié à la sécurisation des grands systèmes de missions [21] et un autre guide dédié à la sécurisation des systèmes embarqués critiques [22]. Les deux guides ont en commun une échelle à cinq niveaux, où :

- le niveau le plus bas correspond au jeu de mesures obligatoires, même si l'appel d'offre ne contient aucune exigence en matière de cybersécurité ; les mesures protègent contre des violations de sécurité occasionnelles ou fortuites ;

| Axe | Thématique | IE PUID | Libellé | D1 | D2 | D3 | D4 | I1 | I2 | I3 | I4 | C1 | C2 | C3 | C4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Protection | Identification et authentification | PROT-IDAUTH-6 | Authentification multifacteur | | | | | | | | O | | | | O |
| Protection | Identification et authentification | PROT-IDAUTH-8 | Protection des informations d'authentification | | | | | O | O | O | O | | O | O | O |

Figure 7 : Extrait du référentiel de sécurité de la SSI Thales

- le niveau 2 correspond aux mesures à mettre en place si la perte de confidentialité, d'intégrité ou de disponibilité est susceptible d'avoir un effet négatif limité sur les opérations de l'organisation, les actifs ou les individus ; les mesures protègent contre une violation intentionnelle de la sécurité en utilisant des moyens simples avec de faibles ressources, des compétences génériques et une faible motivation ; par conséquent, les mesures concernent des solutions bon marché, en termes de coûts récurrents, non récurrents, de développement, d'installation et/ou de maintenance ;
- le niveau 3 correspond aux mesures à mettre en place si la perte de confidentialité, d'intégrité ou de disponibilité est susceptible d'avoir un effet défavorable sérieux ; les mesures protègent contre une violation intentionnelle de la sécurité en utilisant des moyens sophistiqués avec des ressources modérées, des compétences spécifiques et une motivation modérée ; par conséquent, les mesures soutiennent une certaine forme de défense en profondeur (deux niveaux) ;
- le niveau 4 correspond aux mesures à mettre en place si la perte de confidentialité, d'intégrité ou de disponibilité est susceptible d'avoir un effet négatif grave ou catastrophique ; les mesures protègent contre une violation intentionnelle de la sécurité en utilisant des moyens sophistiqués, avec des ressources étendues, des compétences spécifiques et une forte motivation ; les mesures comprennent des solutions potentiellement coûteuses, typiquement des produits certifiés ; ces mesures implémentent de la défense en profondeur (jusqu'à trois niveaux).
- le niveau 5 correspond à ce qui se fait de mieux en matière de cybersécurité, y compris parfois des prototypes de laboratoire ; le fait de lister ces mesures, même si elles ne sont pas encore matures, permet aux concepteurs de concevoir leurs systèmes à longue durée de vie afin que ces techniques innovantes soient facilement intégrables à court ou moyen termes, lorsqu'elles seront disponibles.

Cette approche a été encore raffinée au sein de certains secteurs d'activités du Groupe Thales, par exemple pour certaines lignes de produits de Thales Land and Air Systems [38].

Une bonne adéquation du référentiel au domaine d'application permet de réduire significativement le nombre de risques qui seront éventuellement identifiés lors de l'analyse de risque par scénario.

## 3.7. ISO/CEI 27k

L'ISO/CEI dispose d'un référentiel de mesures de sécurité avec ISO/CEI 27002 [2] et d'un processus de gestion des risques avec l'ISO/CEI 27005 [3]. Même si le §8.1 de la norme ISO/CEI 27005 indique qu'il faut identifier les mesures de sécurité existantes et leurs effets sur le risque identifié, il ne s'agit pas à proprement parlé d'une démarche de détermination d'un socle de sécurité préalable à l'évaluation des risques de sécurité.

Le principe de détermination préalable d'un socle de sécurité a été discuté pour la prochaine édition de l'ISO/CEI 27005, attendue pour la fin 2022, mais la norme ne proposera pas une manière précise pour constituer ce socle. Néanmoins, l'ISO/CEI 27005 étant une norme de la famille 27xxx, elle bénéficie du soutien en la matière de l'ISO/CEI 27002.

L'ISO/CEI 27002 est également en cours de révision, prévue pour 2022. Elle devrait proposer des mesures de sécurité additionnelles tout en proposant, par mesure de sécurité, des paramètres pour faire le lien vers d'autres standards. Ces paramètres sont, de manière non exhaustive, le lien avec les critères de sécurité (D-I-C), les types de contrôles (préventif, correctif, etc.), les différentes catégories du NIST (Identifier, Protéger, Détecter, etc.), ou les domaines de sécurité de l'ENISA [11]. Cette matrice de traçabilité est primordiale pour automatiser un suivi de conformité d'un socle de sécurité multi-référentiels. Une fois disponible, cette norme devrait fournir une pierre angulaire pour l'établissement d'équivalences

entre les référentiels. Un socle pourrait ainsi être automatiquement adapté en fonction du référentiel applicable par contrat, sans pour autant changer les mesures de sécurité du socle.

## 4. Discussion

Dans les méthodes hybrides, l'étape de détermination du socle de sécurité se doit d'être simple et accessible à tous les ingénieurs et architectes système, y compris ceux qui ne sont pas spécialisés en cybersécurité. Ce travail doit pouvoir être réalisé en quelques heures, sans connaissance particulière en cybersécurité, et très tôt dans le cycle de vie du système[4]. Il ne doit nécessiter aucune connaissance particulière sur l'architecture du système. Au contraire, il doit permettre de poser un premier cadre de prise en compte de la sécurité dès les phases initiales du développement système. Cette étape est aussi, par essence, la plus propice à une automatisation. Elle se doit d'être suivie par une étude d'analyse de la conformité du SI au socle, et d'une étape de sécurisation par scénarios, notamment s'il y a des non-conformités.

### 4.1. De la détermination du socle à l'étude de conformité

Pour déterminer un socle de sécurité au juste besoin et proportionné aux enjeux, la clé de voûte est l'étape préliminaire de catégorisation du système à sécuriser. Nous avons montré que les différentes approches internationales (cf. chapitre 3) offrent une grande diversité pour cette étape. Elle peut être basée :

- sur les besoins,
- sur les enjeux,
- sur le niveau attendu des cyberattaques,
- ou encore sur une combinaison de deux ou trois de ces dimensions.

Le rapport sur la maturité en matière de sécurité des systèmes d'information [39] de l'ex-Direction Centrale de la Sécurité des Systèmes d'Information (maintenant ANSSI) poursuit un objectif autre que la définition d'un socle de sécurité pour sécuriser un système par conformité. Cependant, il se rapproche de ce sujet en ce qu'il décrit brièvement :

- une démarche pour déterminer le niveau de maturité SSI cible d'une organisation, pour que ce niveau soit en adéquation avec les véritables enjeux SSI de l'organisation ;
- une démarche pour déterminer le niveau réel de maturité SSI de l'organisation ;
- une démarche pour permettre à l'organisation d'atteindre le niveau adéquat.

Pour déterminer le niveau adéquat de maturité SSI d'une organisation en fonction de ses enjeux SSI, l'approche, qui s'inspire de l'ISO/CEI 21827 [40], propose de répondre à douze questions (cf. Figure 8) concernant :

- les besoins de sécurité, selon les trois critères de D-I-C, dont nous avons vu qu'ils déterminaient l'essentiel des mesures de sécurité fonctionnelles du socle de sécurité (cf. §2.1 et §2.3) ; nous avons en particulier vu que ces besoins étaient finement gérés dans les approches de la NSA (cf. §3.3), de l'ISA/CEI 62443 (cf. §3.5), avec son vecteur de niveaux de sécurité, ainsi que dans celle de la SSI Thales (cf. §3.6) ;
- les conséquences du non-respect des besoins (cf. §2.2 et §2.3), sachant que nous avons vu que la gravité de ces conséquences sont à la base de la détermination du socle de sécurité selon les approches du NIST (cf. §3.2), de la NSA (cf. §3.3), et dans une moindre mesure de l'IT-Grundschutz (cf. §3.4) ;
- le degré d'exposition aux menaces, sachant que nous avons vu que le niveau de cyberattaques est à la base de la détermination du socle de sécurité selon les approches d'EBIOS - Risk Manager (cf. §3.1), de l'ISA/CEI 62443 (cf. §3.5), et, dans une moindre mesure, de l'IT-Grundschutz (cf. §3.4) et du NIST SP800-172 (cf. §3.2).
- l'importance des vulnérabilités, notamment pour les systèmes dont l'organisation souhaite assurer le maintien en condition de sécurité.

Il est intéressant (et logique) de voir que l'on retrouve ici toutes les dimensions discutées dans ce papier, et utilisées dans les différentes normes et différents standards pour définir un socle de sécurité. A ces dimensions, s'ajoute l'importance des vulnérabilités.

[4] Y compris en phase de réponse à appel d'offre, alors que l'architecture n'est pas encore définie. Cette approche permet de remplir la réponse à l'appel d'offre à peu de frais, et d'établir une première cotation du coût de la sécurisation du système.

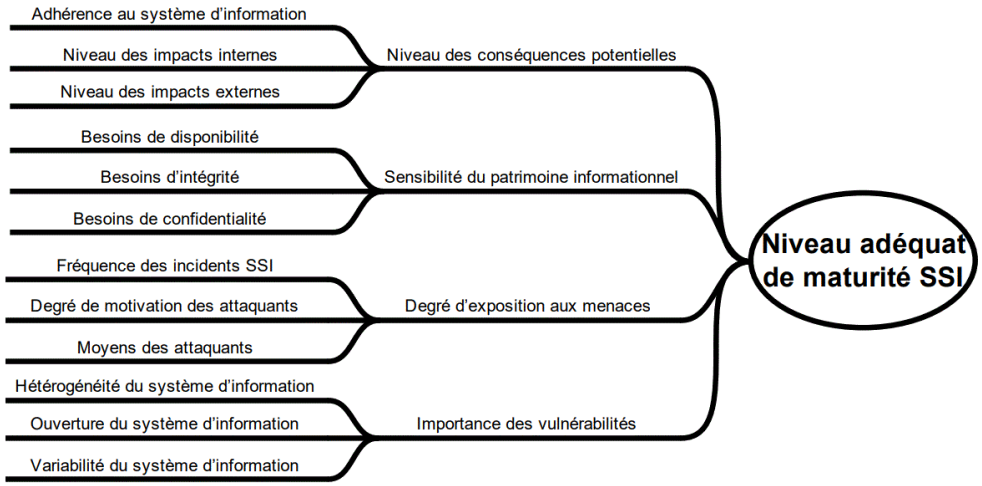


Figure 8 : Douze questions pour estimer le niveau adéquat de maturité SSI

Dans les démarches hybrides que nous avons étudiées, l'hétérogénéité, l'ouverture et la variabilité du SI (c'est à dire l'importance des vulnérabilités, au sens de l'ANSSI), ne sont pas des dimensions servant directement à la sélection d'un socle de sécurité. Cependant, chaque mesure d'un socle de sécurité est de fait établie pour couvrir une ou plusieurs vulnérabilités potentielles. Il est implicite que la sécurisation par conformité comporte deux grandes activités :

- la détermination du socle de sécurité (objet de cette publication), puis
- l'étude de la conformité (du système réel) à ce socle de sécurité.

Cette dernière activité est indispensable. Il est en effet très rare, voire hypothétique, qu'un socle de sécurité puisse être parfaitement implémenté, qu'il opère exactement comme prévu et qu'il produise tous les effets désirés. De fait chaque écart constaté peut (et même devrait) être exprimé sous forme d'une ou plusieurs vulnérabilités concrètes et exploitables.

Ce sont autant de vulnérabilités qui seront amenées à alimenter les scénarios d'attaque de la phase d'analyse des risques par scénarios. L'analyse par scénario permet de statuer sur l'acceptation des vulnérabilités, ou sur leur couverture, par une mise en conformité directe, ou par des mesures de sécurité complémentaires et compensatoires. Par contraste avec la tâche de sécurisation par conformité, cette tâche de consolidation ou d'enrichissement du socle de sécurité est réalisée par un spécialiste en cybersécurité. Elle nécessite en effet une bonne connaissance des vulnérabilités, e.g. [41], et des techniques d'attaque, e.g. [42]. Elle permet d'affiner le choix des mesures. Ce travail sera d'autant plus facile à réaliser que la présélection du socle de mesures de sécurité aura été finement effectuée.

## 4.2. Standards et outils support à une automatisation

La systématisation, voire l'automatisation, de la détermination d'un socle de sécurité, ainsi que l'analyse de conformité du SI au socle, sont des enjeux permettant à une organisation de gagner en efficacité. Nous avons pu voir au cours de cette publication qu'un ensemble d'étapes peuvent être automatisées par des opérations de filtrage et de manipulation de tableaux recensant un ensemble de mesures de sécurité et de menaces élémentaires associées.

D'autres standards outillés viennent compléter cette approche afin de passer d'une approche basée sur une description des mesures de sécurité de manière textuelle, propriétaire et manuelle à une approche standardisée, automatisable par l'utilisation d'un langage machine et d'un format adapté.

OSCAL – the Open Security Controls Assessment Language [43], est un standard du NIST permettant d'uniformiser le format d'échange de données (XML, JSON, YAML) pour la description et l'implémentation de mesures de sécurité. Son utilisation est actuellement déployée pour de nombreux standards comme le NIST SP800-53, FedRAMP, FISMA, HIPPA, PCI DSS. L'ISO/CEI 27002 est en cours d'adaptation. OSCAL permet, par l'utilisation de différentes couches d'abstraction, d'assurer la sélection,

l'affectation, le suivi de l'implémentation et la conformité des mesures de sécurité au sein d'un système ou d'une organisation. Les mesures de sécurité sont répertoriées en catalogues. L'applicabilité pour un système donné est exprimée sous la forme de profil ou socle de sécurité. L'implémentation et l'évaluation sont assurées par des couches dédiées. On peut aisément s'interroger sur l'intégration de ce type de format avec des outils utilisés pour l'ingénierie système, comme DOORS [44].

OSCAL vient soutenir d'autres initiatives de standardisation de format comme SCAP – Security Content Automation Protocol [45], pour la gestion des vulnérabilités et le suivi des correctifs de sécurité, ou encore OCIL – Open Checklist Interactive Language [46] pour les listes de vérification de durcissement des systèmes.

La limitation de ces approches dans une démarche de détermination d'un socle de sécurité tient dans le fait que ces formats standardisés ne sont pas encore vraiment utilisés dans les outils de gestion de risques. Néanmoins, ceux qui intègrent la notion de socle de sécurité proposent en général des fonctions d'import assez flexibles, ce qui peut permettre leur intégration, après adaptation, au format de leurs bases de connaissances.

## 4.3. Le mappage de standards : un besoin catalyseur d'une automatisation du socle de sécurité ?

Sélectionner un socle de sécurité de manière automatique, et le compléter à la marge manuellement est un premier pas. Malheureusement, c'est rarement suffisant. Avec la multiplication des standards, la tendance actuelle amène à ce que la plupart des systèmes réclament une conformité à plusieurs standards. Typiquement, si vous développez une application de divertissement, les standards de développement vidéo s'appliqueront. Votre application est payante, les standards de gestion de comptes et de systèmes de paiement s'appliqueront. Votre application est hébergée dans les nuages, et un autre lot de standards s'appliquera. Par ailleurs, les standards applicables peuvent également varier en fonction de l'acheteur, ou tout du moins de son pays d'origine. Ainsi, un système développé pour le marché européen pourra se voir réclamer une conformité à d'autres standards s'il est vendu en Amérique, ou en Asie-Océanie.

Une première approche pourrait être de déterminer un par un les socles de sécurité adaptés à chaque combinaison de standards. Cette approche pouvait peut-être s'entendre il y a quelques années en arrière lorsque le nombre de standards applicables aux systèmes d'information était encore faible. Désormais il est illusoire de pouvoir mener à bien une telle approche, de par le nombre de standards actuellement applicables et l'arrivée continue de nouveaux standards, au fur et à mesure de la montée en dépendance de nouveaux secteurs d'activités vis-à-vis des systèmes d'information (p.ex. le secteur automobile aujourd'hui avec la voiture connectée et demain avec la voiture autonome, le secteur aéronautique et spatial avec des vols sans pilotes, etc.) et l'explosion combinatoire qui en résulte en termes de socles de sécurité multistandards !

Une autre option est d'envisager le mappage entre standards. En effet, il existe de nombreuses redondance entre tous les standards. Etre conforme à un standard implique souvent une conformité partielle vis-à-vis d'un ou plusieurs autres standards. Le mappage entre standards permet de déduire automatiquement cette conformité induite, ne laissant qu'une faible part à l'analyse manuelle.

Certains éditeurs de standards fournissent ce mappage d'eux-mêmes, pour quelques standards de référence. Par exemple, le NIST fournit le mappage entre le NIST SP 800-53 et l'ISO/IEC 27001 [47]. De même, la matrice de traçabilité proposée dans la prochaine révision de l'ISO/CEI 27002, comme expliqué au §□, devrait apporter un élément structurant pour la traçabilité multi-référentiels.

Les feuilles Excel sont très utilisées dans la communauté pour mapper les standards entre eux. Cependant, les feuilles Excel atteignent vite leurs limites quand le mappage doit être réalisé entre plus de deux standards. Certains outils de management des risques (e.g., ARM [48]) reprennent à leur compte les principes de mappage sur Excel, en autorisant le mappage des standards deux à deux. Cela permet d'aller un peu plus loin qu'avec Excel, mais comme la transitivité entre standards n'est pas vraiment assurée, chaque ajout de nouveau standard implique un nombre croissant de mappages avec les standards en base.

Pour contourner ce problème, une autre approche consiste à s'appuyer sur un référentiel pivot de mesures de sécurité. Ainsi, chaque nouveau standard est mappé avec le pivot, qui assure ensuite son mappage avec tous les autres standards saisis. C'est le cas du produit CDCAT [49]. La SSI de Thales a également eu cette approche vis-à-vis des réglementations applicables aux SI internes de Thales et s'est pour cela appuyée sur la solution DOORS [44] d'IBM, un outil de gestion d'exigences. Par définition, le référentiel pivot se doit d'être le plus exhaustif possible. Sa constitution initiale demande un réel investissement - de l'ordre d'un semestre a été nécessaire à la SSI de Thales pour l'établir. Ensuite le mappage avec un nouveau référentiel dans l'outil de gestion d'exigences demande de quelques jours à quelques semaines de charge effective. Ce temps de mappage d'un nouveau standard est directement lié à la taille du pivot. APMG International annonce ainsi des temps de l'ordre de trois à six semaines pour son outil CDCAT. Ensuite, la génération d'un socle de sécurité multistandards se limite à une simple requête dans l'outil. Dans ce contexte, le maintien de manière centralisée du référentiel pivot sera un gage de sa pérennité dans le temps.

Un point très structurant dans cette approche est le choix du niveau de granularité du référentiel pivot. En effet tous les standards actuellement en circulation n'ont pas un niveau de granularité homogène, entre ceux d'assez haut niveau comme les ISO-27001 & 27002 et ceux très précis comme l'IT Grundschutz Kompendium [13] du BSI ou encore les standards du MITRE [42] et du NIST [10], etc. Le niveau de granularité à adopter pour le référentiel pivot est le facteur prépondérant sur l'effort à fournir pour le travail préparatoire de détermination du référentiel pivot.

## 5. Conclusion

Nous avons défini le besoin de sécurité comme la tolérance maximale qu'une organisation peut s'autoriser sur les différents critères de sécurité (i.e. disponibilité, intégrité et confidentialité) vis-à-vis de ses valeurs métier avant de sortir d'un fonctionnement nominal, voire de rentrer en gestion de crise. Nous avons défini le franchissement de cette ligne rouge comme un événement redouté. Nous avons montré que le niveau d'impact des conséquences de ce franchissement de ligne rouge permettait de définir la gravité de l'événement redouté de façon objective. Nous avons insisté sur le fait qu'il ne fallait pas confondre le niveau du besoin de sécurité, et la gravité de l'événement redouté associé, car la distinction entre ces notions est essentielle à l'automatisation de la détermination d'un socle de sécurité ajusté. Le niveau du besoin de sécurité guide la sélection des mesures de sécurité fonctionnelles ; le niveau des enjeux guide le choix des mesures de sécurité non-fonctionnelles.

Dans un second temps, nous avons montré que les normes et standards de cybersécurité récents préconisent des démarches hybrides. Tout d'abord une approche de la sécurisation par conformité, au juste besoin et proportionnée aux enjeux et/ou aux menaces, qui repose sur la détermination d'un socle de sécurité. Puis une approche itérative consistant à enrichir si besoin ce socle par l'analyse détaillée de scénarios d'attaque, notamment concernant les menaces persistantes avancées (APT).

Nous avons montré que la sécurisation par conformité au juste besoin traite l'essentiel du problème de la sécurisation, et qu'elle peut souvent être menée en autonomie par des experts métiers, c'est à dire sans le support d'un spécialiste en cybersécurité. En effet, une fois le référentiel choisi (e.g. BSI Standard 200-2 [34], NIST SP 800-53B [27], ISA/CEI 62443 [14] ou profils ad-hoc tels que les profils de Thales [21] [22]), le processus est simple, uniquement basé sur une analyse du besoin et un bonne connaissance du métier. Ce dernier point comprend la compréhension des enjeux et/ou le niveau attendu de cyberattaques. Ces étapes sont encore relativement manuelles, y compris dans les grands groupes comme Thales, mais l'analyse faite dans ce papier montre que le potentiel pour une automatisation est réel lorsque les notions en jeu sont bien comprises.

Au-delà de la détermination du socle, nous avons aussi évoqué l'importance de l'étude de la conformité du système au socle. Chaque écart constaté est assimilable à une vulnérabilité qui doit être traitée lors de l'étude complémentaire d'analyse de risque par scénarios. Cette dernière activité, complémentaire à l'activité de sécurisation par conformité, est quant à elle menée par des spécialistes en cybersécurité. De ce fait, la sécurisation selon les approches hybrides devient l'affaire de tous, et pas seulement des spécialistes en cybersécurité.

Enfin, nous avons évoqué quelques outils qui peuvent venir en soutient à cette automatisation de la détermination de socles de sécurité. Malgré l'émergence de ces standards outillés, le chemin vers une automatisation avancée (i.e., autre que l'automatisation d'un simple regroupement d'exigences) s'annonce long et complexe. Un sondage récent au sein de Thales a permis d'identifier 105 standards clefs pour les métiers du Groupe, et cette liste est probablement encore incomplète. Le potentiel d'automatisation et de mappage entre standards devra être étudié avant d'investir sur une automatisation concernant certains de ces standards. Le point clé pour permettre une avancée conséquente dans ce domaine est le partage des bases de connaissances et matrices de traçabilité au sein de la communauté scientifique. Ce facteur est le plus limitant car, à l'heure actuelle, les initiatives de constitution de socles de sécurité sont souvent faites de manière individuelle et isolée, où chacun réinvente la roue. Il nous faut maintenant capitaliser sur des travaux précédents, focaliser les efforts sur l'avancée des techniques d'automatisation, ainsi que sur leur outillage.

## 6. Remerciements

Ce papier a été partiellement financé par les projets Européens FORESIGHT (réf. 833673) et PRAETORIAN (réf. 101021274).

## 7. Références

[1] Department of Trade and Industry (DTI), Code of Practice for Information Security Management', London: British Standards Institute (BSI), 1992.

[2] ISO/CEI 27002, Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information, Edition 2 éd., Organisation Internationale de Normalisation / Commission Electrotechnique Internationale, 2013, p. 88.

[3] ISO/CEI 27005, Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information, Organisation Internationale de Normalisation / Commission Electrotechnique Internationale, Juin 2011, p. 77.

[4] NIST SP800-30 rev. 1, «Guide for Conducting Risk Assessments,» National Institute of Standards and Technology, Gaithersburg, USA, 09/2012.

[5] CLUSIF, «Les fondamentaux de MÉHARI,» Club de la Sécurité de l'Information Français, [En ligne]. Available: https://clusif.fr/services/management-des-risques/les-fondamentaux-de-mehari/. [Accès le 03 02 2021].

[6] M. A. Amutio, J. Candau and José Antonio Mañas, MAGERIT – Methodology for Information Systems Risk Analysis and Management, Madrid, Spain: Ministry of Finance and Public Administration, July, 2014.

[7] ANSSI, «La méthode EBIOS Risk Manager - Historique & héritage d'EBIOS RM,» Agence Nationale de la Sécurité des Systèmes d'Information, 2021. [En ligne]. Available: https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/#. [Accès le 22 01 2021].

[8] BSI Standard 100-2, IT-Grundschutz Methodology, 2.0 ed., Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI), 2008, p. 93.

[9] ISO/CEI 27k, «Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information,» Organisation internationale de normalisation / Commission Electrotechnique Internationale.

[10] NIST SP 800 series, «NIST Special Publication 800-series,» National Institute of Standards and Technology, [En ligne]. Available: https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information. [Accès le 15 01 2021].

[11] ENISA, "Minimum Security Measures for Operators of Essentials Services," European Union Agency for Cybersecurity, [Online]. Available: https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services. [Accessed 27 09 2021].

[12] Journal officiel de l'Union européenne, «Directive (UE) 2016/1148 du Parlement Européen et du conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union,» 19 07 2016. [En ligne]. Available: https://eur-lex.europa.eu/legal-

content/FR/TXT/PDF/?uri=CELEX:32016L1148&from=FR. [Accès le 08 04 2021].

[13] BSI, IT-Grundschutz-Kompendium, Bonn, Germany: Federal Office for Information Security (BSI), Feb. 2021.

[14] ISA/CEI 62443, « Réseaux industriels de communication - Sécurité dans les réseaux et les systèmes », International Society of Automation / Commission Electrotechnique Internationale.

[15] ANSSI SecNumCloud, « Prestataires de services d'informatique en nuage (SecNumCloud) - référentiel d'exigences », Agence nationale de la sécurité des systèmes d'information (SGDSN/ANSSI), Paris, 11 juin 2018.

[16] ISO/CEI 80001, « Application du management du risque aux réseaux des technologies de l'information contenant les dispositifs médicaux », Organisation internationale de normalisation / Commission Electrotechnique Internationale, 2010.

[17] ISO/SAE DIS 21434, Véhicules routiers — Ingénierie de la cybersécurité, Organisation internationale de normalisation / SAE International, 2020.

[18] PCI, «Les standards de sécurité PCI,» PCI Security Standards Council, 15 01 2021. [En ligne]. Available: https://fr.pcisecuritystandards.org/minisite/env2/.

[19] ANSSI, EBIOS Risk Manager, version 1.1 éd., Paris: Agence Nationale de la Sécurité des Systèmes d'Information, Dec. 2018, p. 49.

[20] NIST FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, Gaithersburg: National Institute of Standards and Technology, 2004.

[21] 87210649-DDQ-GRP-EN, Cybersecurity Guide for Solution Architects, vol. Rev. 2, Thales Chorus 2.0, Thales Group Limited Distribution, Nov. 2020, p. 62.

[22] 87214870-DDQ-GRP-EN, "Cybersecurity Guide for Equipment Architects," Thales Chorus 2.0, Thales Group Limited Distribution, Jan. 2020.

[23] CESG IA BIL, "Extract from HMG IA Standard No.1 - Business Impact Level Tables," 10 2009. [Online]. Available: https://www.shreddingmachines.co.uk/business-impact-tables.pdf. [Accessed 01 2021].

[24] ANSSI, Guide d'hygiène informatique : renforcer la sécurité de son système d'information en 42 mesures, vol. version 2.0, Paris: Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), Janvier 2017, p. 72.

[25] ANSSI, « Réglementation », Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), [En ligne]. Available: https://www.ssi.gouv.fr/administration/reglementation/. [Accès le 20 01 2021].

[26] NIST SP 800-37r2, Risk Management Framework for Information Systems and Organizations - A System Life Cycle Approach for Security and Privacy, Revision 2 ed., Gaithersburg: National Institute of Standards and Technology, 2018, p. 183.

[27] NIST SP800-53B draft, "Control Baselines for Information Systems and Organizations," National Institute of Standards and Technology, Gaithersburg, USA, 07/2020.

[28] NIST SP800-171r2, Protecting Controlled Unclassified Information in Nonfederal Systems, Gaithersburg: National Institute of Standards and Technology, Feb. 2020.

[29] NIST SP800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information - A Supplement to NIST Special Publication 800-171, Gaithersburg: National Institute of Standards and Technology, Feb. 2021.

[30] NIST SP800-53 rev. 5, "Security and Privacy Controls for Information Systems and Organizations," National Institute of Standards and Technology, Gaithersburg, USA, 09/2020.

[31] NIST SP800-53A rev. 4, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations, Building Effective Assessment Plans," National Institute of Standards and Technology, Gaithersburg, USA, 12/2014.

[32] NIST FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, Gaithersburg: National Institute of Standards and Technology, 2006.

[33] CNSS 1253, Security Categorization and Control Selection for National Security Systems, Ft Meade: Committee on National Security Systems (CNSS), National Security Agency (NSA), 2014.

[34] BSI-Standard 200-2, «IT-Grundschutz Methodology,» Federal Office for Information Security (BSI), Bonn, Germany, oct. 2017.

[35] ISO/IEC 27001, Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences, Organisation

internationale de normalisation (ISO) et Commission Electrotechnique Internationale (CEI), 2013.

[36] BSI-Standard 200-3, «Risk Analysis based on IT-Grundschutz, version 1.0,» Federal Office for Information Security (BSI), Bonn, Germany, Oct. 2017.

[37] IEC 62443-3-3, "Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels," International Electrotechnical Commission, 2013.

[38] Wikipedia, « Thales Land and Air Systems », Wikimedia Foundation, 20 08 2020. [En ligne]. Available: https://fr.wikipedia.org/wiki/Thales_Land_and_Air_Systems. [Accès le 12 01 2021].

[39] DCSSI, Maturité SSI : approche méthodologique, Paris: Direction Centrale de la Sécurité des Systèmes d'Information (SGDN / DCSSI / SDO / BCS), Novembre 2007, p. 24.

[40] ISO/CEI 21827, Technologies de l'information — Techniques de sécurité — Ingénierie de sécurité système — Modèle de maturité de capacité (SSE-CMM®), Organisation Internationale de Normalisation / Commission Electrotechnique Internationale, 2008.

[41] NIST NVD, "National Vulnerability Database," National Institute of Standards and Technology (NIST), [Online]. Available: https://nvd.nist.gov/general. [Accessed 03 02 2021].

[42] MITRE, "MITRE ATT&CK," The MITRE Corporation, 2021. [Online]. Available: https://attack.mitre.org/. [Accessed 03 02 2021].

[43] National Institute of Standards and Technology (NIST), "OSCAL - Implementation Layer," U.S. Department of Commerce, 08 04 2021. [Online]. Available: https://pages.nist.gov/OSCAL/documentation/schema/. [Accessed 09 04 2021].

[44] IBM, "Overview of DOORS," IBM, 2021. [Online]. Available: https://www.ibm.com/docs/en/ermd/9.7.2?topic=engineering-requirements-management-doors-overview. [Accessed 09 04 2021].

[45] National Institute of Standards and Technology (NIST), "SCAP - Security Content Automation Protocol," U.S. Department of Commerce, 07 08 2020. [Online]. Available: https://csrc.nist.gov/projects/security-content-automation-protocol/. [Accessed 09 04 2021].

[46] M. Casipe and C. Schmidt, "The Open Checklist Interactive Language (OCIL) - Version 1.0," MITRE, 11 2008. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Security-Content-Automation-Protocol/specifications/ocil/1.0/OCIL_language.pdf. [Accessed 09 04 2021].

[47] NIST Computer Security Division, "NIST SP 800-53, Revision 5 Control Mappings to ISO/IEC 27001," 22 01 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Publications/sp/800-53/rev-5/final/documents/sp800-53r5-to-iso-27001-mapping.docx. [Accessed 07 09 2021].

[48] ALL4TEC Safe & Secure, « Logiciel EBIOS Risk Manager - Agile Risk Manager - Analyses de risques cyber », [En ligne]. Available: https://www.all4tec.com/logiciel-ebios-risk-manager-labellise-agile-risk-manager/. [Accès le 07 09 2021].

[49] APMG International, "CDCAT® - Cyber Defence Capability Assessment Tool," 2020. [Online]. Available: https://apmg-international.com/product/cdcat. [Accessed 07 09 2021].

[50] ISO/CEI 2003, Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Lignes directrices, Organisation internationale de normalisation / Commission Electrotechnique Internationale, 03/2017.

[51] Parlement Européen, «Directive (UE) 2016/1148 du Parlement Européen et du Conseil,» Journal officiel de l'Union Européenne, Bruxelles, 2016.