Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

SOGETI

Tour d'horizon de la sécurité de l'information dans le monde professionel

27 Janvier 2017

Yannick Busca

Agenda

1. Sogeti
2. Réponse à Appel d'Offre
3. Sécurité dans les projets

Agenda

1. **Sogeti**
2. Réponse à Appel d'Offre
3. Sécurité dans les projets

Le Groupe Capgemini

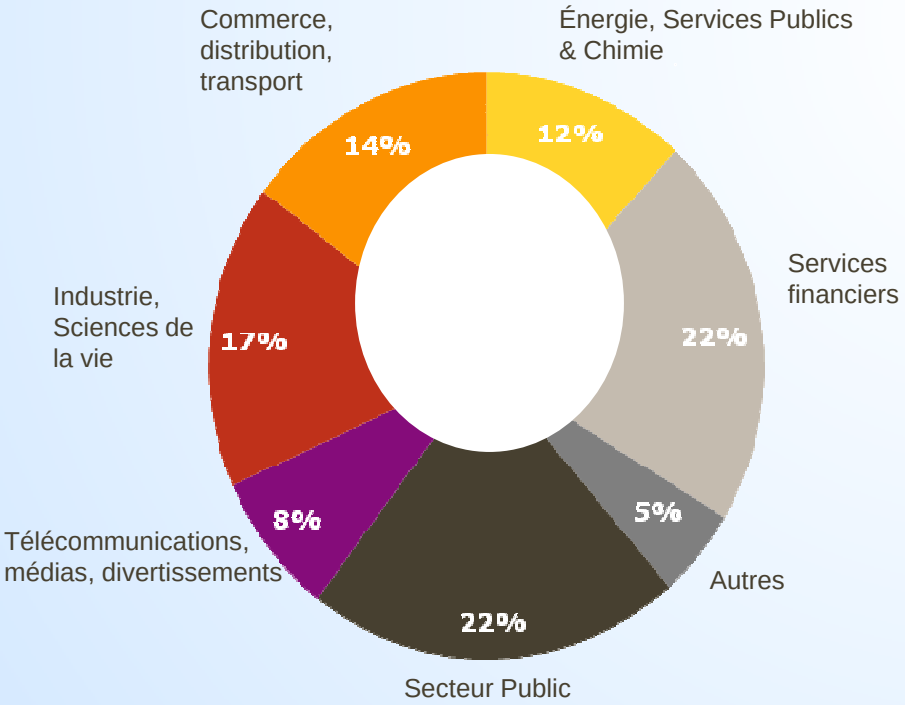
Capgemini, créé en 1967, est l'un **des leaders mondiaux** du conseil en management et des services informatiques.

CA 10, 573 Milliards d'euros

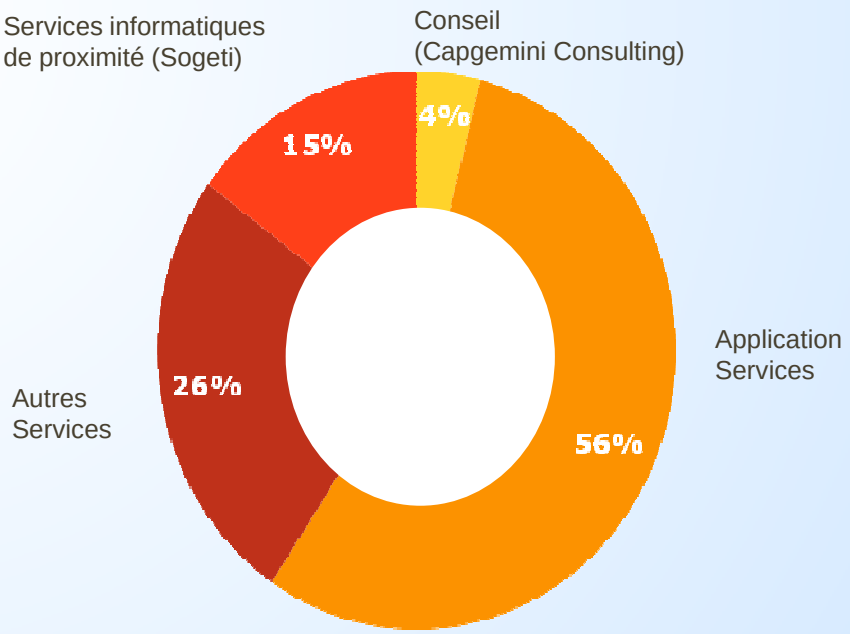
40 pays

180 000 collaborateurs dont plus de 50 000 personnes en offshore*

Revenu par secteur



Revenu par métier



SOGETI en quelques chiffres ...

20 000

COLLABORATEURS
dans le monde

CHIFFRE D'AFFAIRES 2014
Sogeti

1,6 milliard d'euros

100 IMPLANTATIONS
dans 15 pays

en Europe,
aux Etats-Unis et en Inde

6 000
COLLABORATEURS

21
IMPLANTATIONS

Une présence et un delivery distribués

19 VILLES

21
IMPLANTATIONS

1 CENTRE DE SERVICES INDUSTRIEL
3 sites : Pau, Pessac, Toulouse

2 CENTRES OFFSHORE
Inde (Mumbaï, Bangalore, Chennaï,…)
Maroc (Rabat, Casablanca).

CAPACITES INDUSTRIELLES
répondant aux attentes de proximité, d'appropriation des enjeux business et de transformation.

SUR SITE CLIENTS
maintien d'une expertise forte, y compris pour des prestations réalisées massivement en Centre de Services ou en RightShore®.

COORDINATION GLOBALE
assurée par la Direction du Delivery et de la Qualité.

4 domaines et 6 offres stratégiques

Digital	Testing	Sécurité	Infrastructure

Digital
Mobility & Workplace

Digital
Insights & Data

Testing
Testing Services

Sécurité
Cybersecurity

Infrastructure
Data Center Transformation et Cloud

Infrastructure
Infrastructure Management

Services de conseil opérationnel et stratégique
Services d'audit de sécurité

Conseil stratégique en cybersécurité

- Evaluation du niveau de maturité et d'hygiène
- Transformation de l'organisation cybersécurité et professionnalisation
- Sensibilisation et gestion du changement
- Classification & protection des données / vie privée / fuite de données

Conseil opérationnel

ISO 27001, IEC 62443
ANSSI, CESG, BSI, NIST

- Définition du périmètre à sécuriser
- Cartographie des installations matérielles, des systèmes et des applications critiques
- Classification : différents niveaux de criticité, de sûreté, de disponibilité ou d'intégrité attendus
- Analyse de risques
- Définition des objectifs de sécurité
- Procédures/mesures de sécurité (organisationnelles et techniques)

Services d' Audit

- Tests d'intrusion système
- Test de sécurité des applications – « As-a-Service »
- Investigations numériques
- Audit de Sécurité (organisation, configuration, architecture)
- Conformité règlementaire

Points forts de la *Business Line* Sécurité

- Labellisé « Prestataire de Confiance pour les Audits de Sécurité **(PASSI)** » par l'ANSSI;
- Retenu dans le cadre de la démarche de Détection des Incidents de Sécurité (**PDIS**) défini par l'ANSSI;
- Souhaite s'inscrire dans la démarche de prestataire de réponse et d'investigation sécurité (**PRIS**) en 2016;
- Habilité Centre d'Evaluation de la Sécurité des Technologies de l'Information (**CESTI**), par l'ANSSI, et d'un Institut de formation habilité par le LSTI pour délivrer les formations et examens certifiants ;

- Labellisé « **France Cybersécurité** » pour les audits de sécurité et le SOC
- Membre du **Club des Prestataires de Confiance** fondé sur l'impulsion de l'ANSSI (4 sociétés uniquement);

- SOGETI dispose d'un SOC dans ses locaux de Toulouse
- SOGETI dispose d'un CERT opérationnel depuis le 1er Septembre 2015 et labélisé au TF-CSIRT (TI)

L’intervenant

CRYPTIS

10 ans d’expérience

Paris Toulouse

Capgemini Lexsi Sogeti

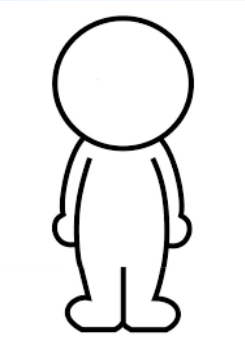
Type de missions	Domaine sectoriel
Audits sécurité/maturité	Bancaire, Défense, Energie, Public, Service, Transport, Santé, Industrie
Sécurité et infogérance (cloud …)	Défense, Banque, Industrie, Service
PKI / IGC	Luxe, Banque
Sécurité dans les projets	Défense, Energie, Banque
Indicateurs, Tableaux de bords	Public
Roadmap / stratégie sécurité	Public, Evènementiel, Industrie, Service
Politiques, procédures	Service
Analyse de risques	Bancaire, Défense, Industrie, Public
Gestion d’équipes / budgets	Service

Agenda

1. Sogeti
2. **Réponse à Appel d'Offre**
3. Sécurité dans les projets

Réponse à Appel d'Offre

Dans la vie courante



Quel produit / service?

Quel besoin ?

- ✓ Pour quel usage ?
- ✓ Combien de kilomètres / an ?
- ✓ Quelle couleur ?
- ✓ Quelle puissance ?
- ✓ Quelle finition ?
- ✓ Coût d'assurance ?
- ✓ Entretien ?

Réponse à Appel d'Offre

Un Appel d'Offre ?

- La description d'un besoin
- B2B
- One Shot / récurrent
- Produit et/ou service (conseil, intégration, développement, service récurrent, licences …)
- Règlementé (pays, public/privé)

Réponse à Appel d'Offre

Comment est-ce formalisé ?

- Cahier des clauses techniques particulières (CCTP)
- Conditions Générales d'Achat ou de Vente (CGA/CGV)
- Un email … un RDV

Réponse à Appel d'Offre

Comment y répond t'on ?

➡ Une proposition commerciale (V1, V2, …)

- Rappel du contexte ;
- Rappel des enjeux et des objectifs ;
- Démarche proposée (activités, livrables) ;
- Equipe / planning ;
- Gestion de projet / qualité ;
- Prix et conditions de vente ;

Le fournisseur formalise le besoin et les enjeux associés

Le fournisseur a découpé son offre en étapes « logiques » répondant au besoin – une étape = un ou plusieurs livrables

Le fournisseur propose des ressources adaptées et une démarche de gestion de projet

…. et un prix de vente, conditions de facturation

Réponse à Appel d'Offre

Comment y répond t'on ?

- Une ou des soutenances
- De la négociation (technique, financière, design to cost, …)
- Un contrat, un bon de commande

Réponse à Appel d'Offre

Comment le gagne t'on ?

- En comprenant le besoin (et son client) !!!
- En formalisant une proposition qui y répond clairement et avec la méthodologie appropriée !!
- Avec la bonne équipe, les bons produits, et les bonnes références
- Et au juste prix !!!

Réponse à Appel d'Offre

Qui est impliqué ?

Côté client

- le ou les métiers (IT compris);
- la sécurité ;
- les achats ;
- les juristes ;

Côté fournisseur(s)

- le commerce ;
- l'avant vente ;
- les juristes ;

Réponse à Appel d'Offre

En synthèse

1 – Expression du besoin (RFI, RFP)

2 - Envoi aux soumissionnaires

3 - Réponses techniques et financières

4 - Soutenances et négociation

5 - Sélection du prestataire

6 - Contractualisation

Un exemple de proposition commerciale

1. Enjeux
2. Présentation de la démarche proposée
3. Organisation de la prestation
4. Prix

Enjeux

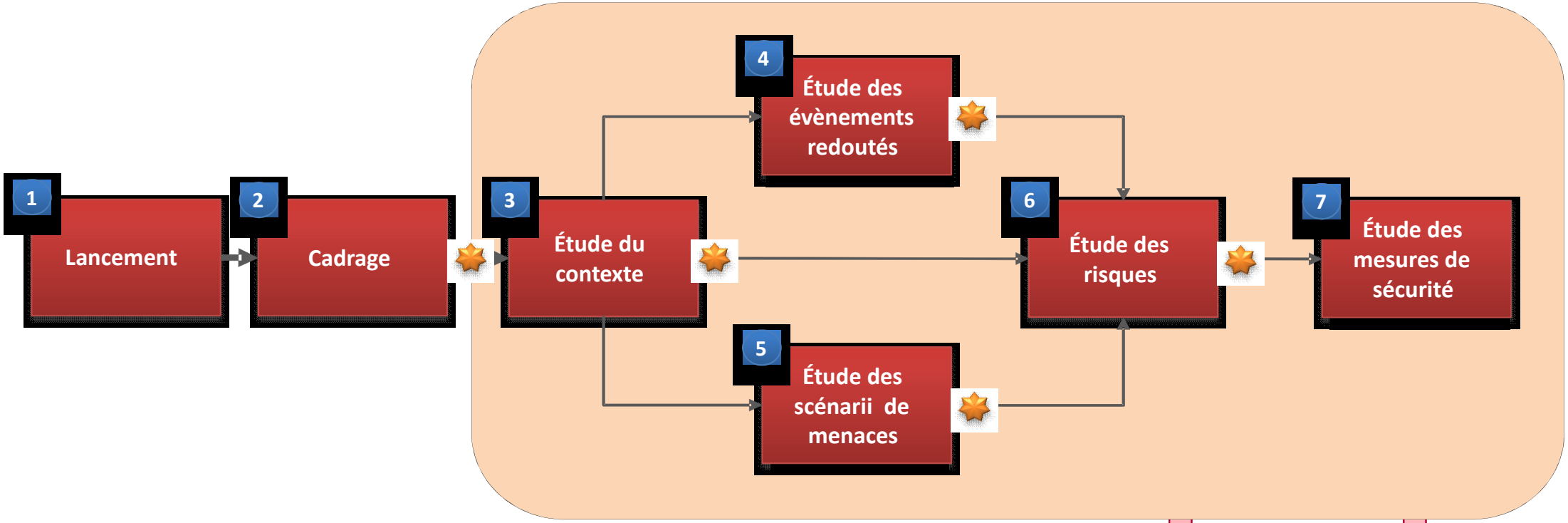
Dans le cadre de la règlementation, LE CLIENT souhaite se faire accompagner dans la réalisation d'une analyse de risques pragmatique sur un système d'information sensible afin de déterminer les mesures de sécurité à mettre en place dans le cadre de cette règlementation et de **lancer rapidement** leur mise en œuvre.

Cette analyse de risques n'a pas pour vocation d'être reprise « telle quelle » dans le dossier d'homologation, mais a pour objectif de **très rapidement** :

1. choisir le mode de traitement des risques identifiés durant l'analyse ;
2. pour les risques à traiter, identifier les mesures de sécurité à mettre en place – ces mesures seront sélectionnées dans un référentiel qui reste à discuter ;
3. sélectionner et lancer les programmes (répondant aux mesures) afin que leur mise en œuvre soit compatible avec les contraintes temporelles imposées par la règlementation (la prestation se limite à la sélection et validation des mesures de sécurité).

Table des matières

Présentation de la démarche proposée



Étape principale de validation

- **Rapports d'analyse de risques du SI ;**

Étude du contexte

- Identification et appropriation du SI;
- Définition des dispositions & métriques de l'analyse de risques ;

Démarche

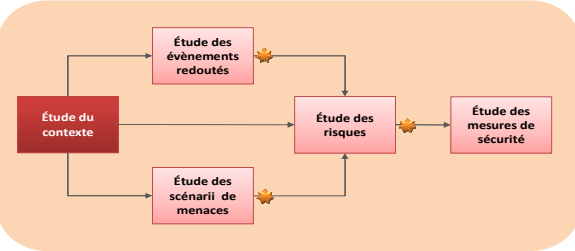
- Intégration des paramètres à prendre en compte:
  - ✓ Enjeux stratégiques, opérationnels et réglementaires,
  - ✓ Contraintes fonctionnelles, techniques et réglementaires,
  - ✓ Hypothèses,
  - ✓ Parties prenantes: autorités, opérateurs, ….
- Etude des dossiers de spécifications fonctionnelles et techniques, de la documentation technique relative à l'existant,
- Identification (cartographie) :
  - ✓ des biens essentiels (processus métiers, fonctionnalités, informations et données),
  - ✓ des biens supports (sites, servitudes, infrastructures IT, personnels),
  - ✓ des mesures de sécurité existantes,
- Sélection des sources de menaces (humaines ou non, intentionnelles ou accidentelles),
- Analyse des mesures de sécurité existantes et/ou des vulnérabilités identifiées lors d'audits,
- Prise en compte ou définition des métriques : paramètres et échelles pour la caractérisation et l'évaluation des risques (besoins sécurité, impacts/gravité, vraisemblance et niveaux de risques).

Interlocuteurs

- Directeur / chef de projet
- Interlocuteur sécurité projet
- Tiers (…)

Limites / hypothèses

- Une grille d'impact/gravité existe, pas de grille de vraisemblance / niveaux de risque / besoins de sécurité
- La liste des sources de menaces EBIOS 2010 sera utilisée



Étude du contexte

Pré-requis

- Descriptif organisationnel des parties prenantes ;
- Dossier de spécifications fonctionnelles, techniques et de sécurité du SI et des applications qui le composent ;

Production

- Liste des biens essentiels du SI (fonctionnalités métiers, données)
- Liste des biens supports du SI (cartographie technique)
- Liaisons entre les biens essentiels et les biens supports (chaîne fonctionnelle / technique)
- Inventaire des sources de menaces retenues et justifiées
- Métriques de gestion des risques validées

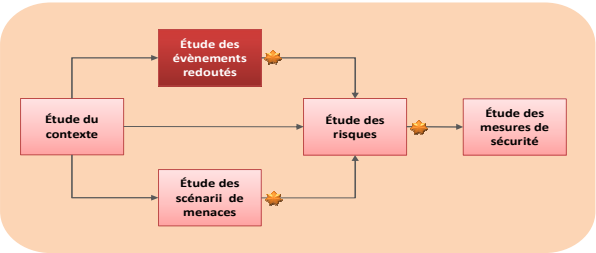
Étude des événements redoutés

Objectifs

- Analyser et quantifier les enjeux de sécurité du SI / des 3 applications qui le composent ;

Démarche

- Identification et analyse des évènements redoutés auprès de la MOA (sur la base d'entretiens individuels), pour chaque bien essentiel :
  - ✓ Des besoins de sécurité (CIDT),
  - ✓ Des impacts occasionnés en cas de sinistre et évaluation de la gravité associée,
  - ✓ Des sources de menaces susceptibles d'en être à l'origine.
- Evaluation des évènements redoutés (hiérarchisation, exclusion éventuelle),
- Validation des besoins de sécurité et des événements redoutés.



Interlocuteurs

- Interlocuteur sécurité projet
- MOA

Limites / hypothèses

- Il y a 3 applications qui composent ce SI donc 3 interlocuteurs métiers – 2 entretiens de travail de 2H par interlocuteur + 1 réunion de restitution collégiale ; au total 7 entretiens métiers
- 10 biens essentiels seront considérés au maximum sur l'ensemble du SI ;

Étude des événements redoutés

Pré-requis

- Liste des biens essentiels du SI / des applications qui le composent ;
- Inventaire des sources de menaces retenues et justifiées ;
- Métriques de gestion des risques validées (cf étape Etude du contexte) ;

Production

- Liste des biens essentiels du SI
- Liste hiérarchisée des évènements redoutés en fonction de leur gravité / impact

Étude des scénarios de menaces

Objectifs

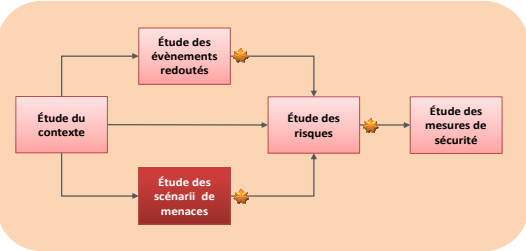
- Identifier et analyser les modes opératoires ou les évènements extérieurs qui pourraient porter atteinte à la sécurité du SI ;

Démarche

- Étude des sources de menaces et de leurs vraisemblances en tenant compte des vulnérabilités exploitables sur les biens supports,
- Validation des scénarios de menaces et de la valorisation de leur vraisemblance .

Interlocuteurs

- MOE
- Interlocuteur sécurité projet



Limites / hypothèses

- Les biens supports composant le SI sont connus et documentés (document d'architecture technique, procédure d'exploitation …) ;
- Pour l'ensemble du SI 10 biens supports maximum seront étudiés ;
- Des rapports d'audit(s) portant sur le périmètre étudié (d'architecture, pentest, configuration) sont disponibles ;
- 4 réunion de travail de 2H avec les équipes MOE en charge du SI + 1 réunion de validation des niveaux de vraisemblance ;

Étude des scénarios de menaces

Pré-requis

- Liste des biens supports ;
- Inventaire des sources de menaces retenues et justifiées ;
- Métriques de gestion des risques validées (vraisemblance) ;

Production

- Liste hiérarchisée et justifiée des scénarios de menaces en fonction de leur vraisemblance

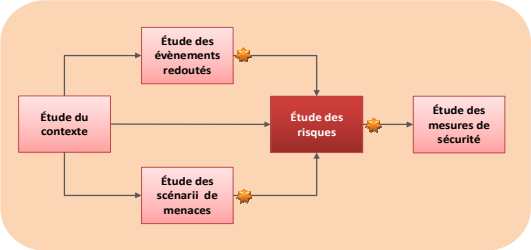
Étude des risques

Objectifs

- Appréciation des risques du SI ;
- Qualification des modes de traitement des risques ;

Démarche

- Analyse des scénarios de risques établis à partir des événements redoutés et des scénarios de menaces précédemment appréciés sur chaque bien essentiel/bien support,
- Identification des objectifs de sécurité pour le traitement des risques (réduction, acceptation, refus, transfert),
- Identification des risques à traiter et des risques résiduels.



Interlocuteurs

- Directeur(s) (ayant la légitimité pour décider du mode de traitement de chacun des risques et d'implémenter les mesures de sécurité sélectionnées)
- Interlocuteur sécurité projet

Limites / hypothèses

- 1 réunion de travail de 2H pour préparer la réunion de restitution avec présentation des risques et des mesures de sécurité associées aux risques ;
- 1 réunion de restitution de 2H maximum

Étude des risques

Pré-requis

- Liste hiérarchisée des évènements redoutés ;
- Liste hiérarchisée et justifiée des scénarios de menaces ;
- Métriques de gestion des risques validées (niveau de risques, critère d'acceptation des risques) ;

Production

- Liste hiérarchisée et valorisée des risques

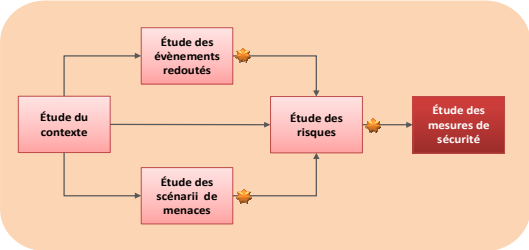
Étude des mesures de sécurité

Objectifs

- Formaliser les exigences de sécurité du SI permettant de traiter les risques ;

Démarche

- Prendre en compte l'ensemble des contraintes réglementaires et de spécifications de sécurité,
- Proposer les mesures de sécurité complémentaires permettant de réduire les risques à un niveau acceptable, si possible.



Interlocuteurs

- Directeur(s) (ayant la légitimité pour décider du mode de traitement de chacun des risques et d'implémenter les mesures de sécurité sélectionnées)
- Interlocuteur sécurité projet

Limites / hypothèses

- 1 réunion de travail de 2H pour préparer la réunion de restitution avec présentation des risques et des mesures de sécurité associées aux risques ;
- 1 réunion de restitution de 2H maximum

Étude des mesures de sécurité

Pré-requis

- Référentiels de sécurité (PSSI Client, règlementations…) ;
- Niveau d'acceptation des risques défini et validé ;

Production

- Fichier excel récapitulant l'ensemble des modules EBIOS (contexte, évènements redoutés, scénarios de menace, valorisation des risques) ;
- Document Word d'analyse de risques « executive summary » statuant les risques, les mesures de sécurité et risques résiduels ;

Table des matières

Organisation pour la gestion et le suivi de mission

- Comitologie
  - Réunion de suivi de 30 minutes 1 fois par mois;
  - Support produit par Sogeti qui servira de base de discussion pendant la réunion de suivi ;

Gestion de projet, communication & sécurité

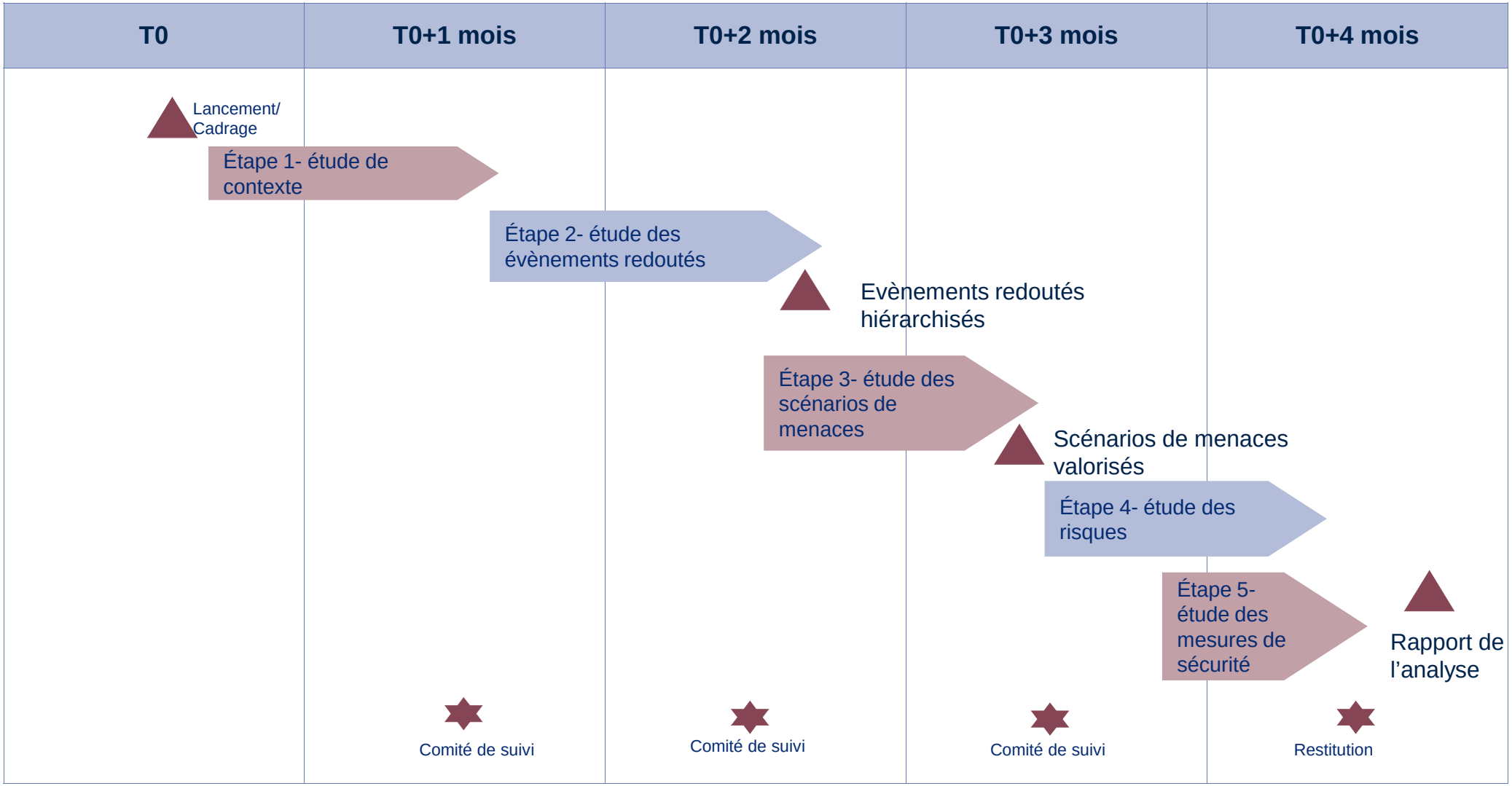
- Les prestations sont réalisées dans les locaux du CLIENT et de SOGETI
- Communication & échanges de documents
  - Échanges chiffrés via une solution appropriée suivant le niveau de sensibilité des documents ;
- Format des livrables : word, excel, ppt & pdf
- Validation des documents
  - Comptes rendus d'entretiens et de réunion : 5 jours
  - Livrables : 2 semaines
  - Procès-verbal de services faits
- Confidentialité
  - Destruction de l'ensemble des données lors de la fin de la prestation après acceptation du PV de réception

Table des matières

Prix

- Rôles, TJM(s), charges (jours/homme, employé temps plein (ETP))
- Prix de vente (incluant la gestion de projet)
- Conditions de facturation
- Engagement de résultat / de moyen

Macro-planning



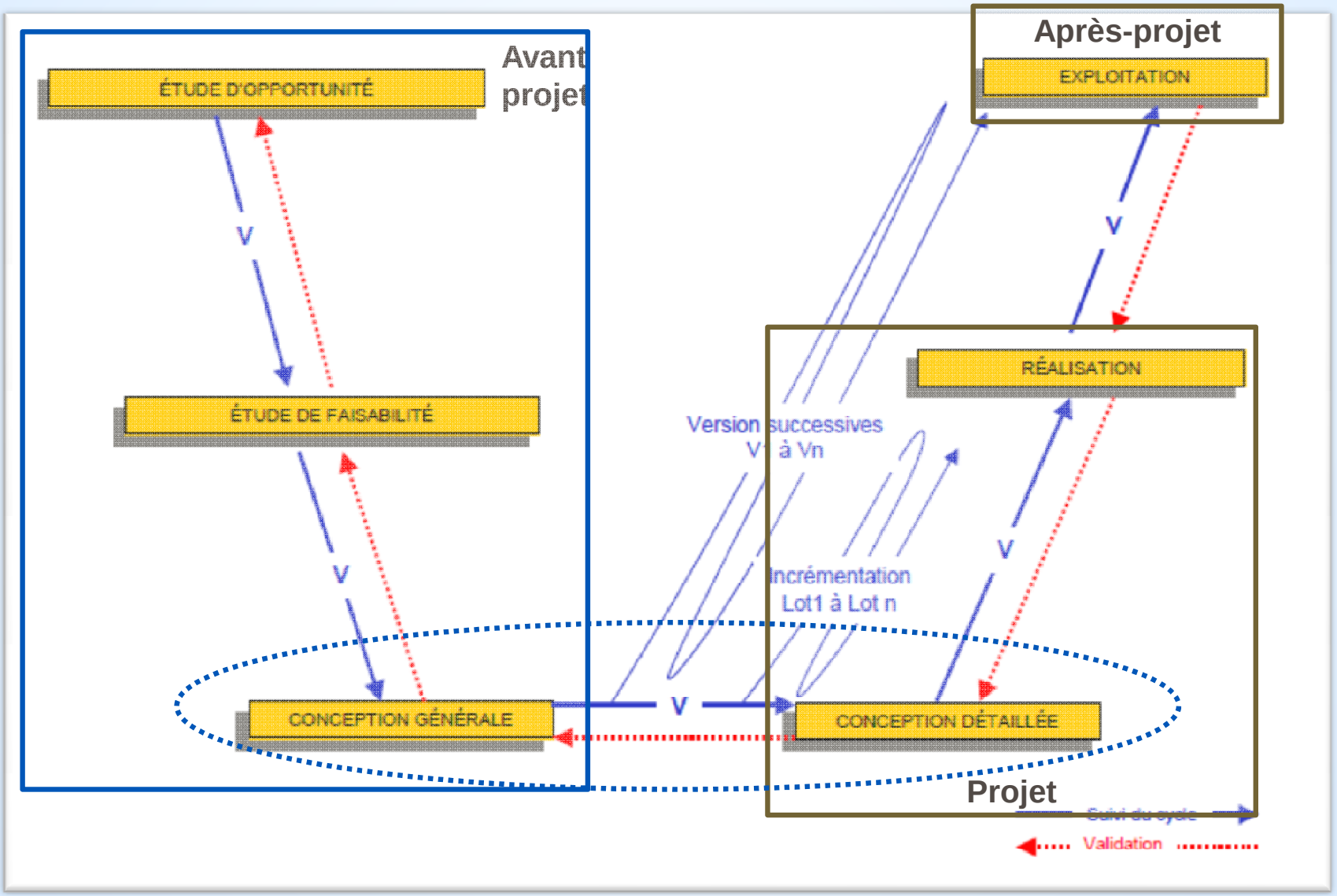
Agenda

1. Sogeti
2. Réponse à Appel d'Offre
3. **Sécurité dans les projets**

Un projet ?

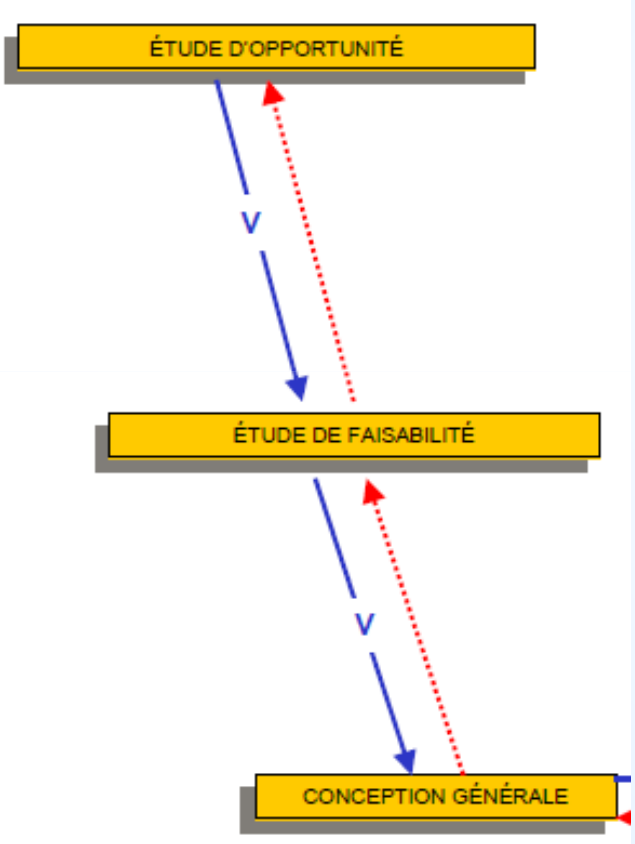
- Une succession d'activités répondant à un besoin exprimé par des parties prenantes et visant à atteindre un objectif précis
- …. dans des délais et un budget définis et maitrisés
- Plusieurs méthodologies projet adaptées à des besoins spécifiques (cycle en V, agile …)
- …. Et après le projet ? ….
- Maintien en condition opérationnelle/de sécurité (RUN, BAU) du « projet »

Les différentes phases d'un projet



GISSIP

Avant projet



Étape 1 – Étude d'opportunité

L'étude d'opportunité vise à définir le cadre potentiel du projet, son intérêt pour l'organisme :
- ❑ analyse et hiérarchisation des **enjeux**,
- ❑ analyse des freins et des leviers (organisation, technologie, culture et motivation),
- ❑ identification et évaluation des ressources internes et externes à mettre en oeuvre,
- ❑ estimation du **retour sur investissement.**

✓ *Dans le domaine de la SSI, cette étape est fondamentale, elle conditionne toute la suite du projet car c'est à ce moment que sont évalués les **grands enjeux SSI du projet** et donc l'investissement consenti pour gérer les risques.*

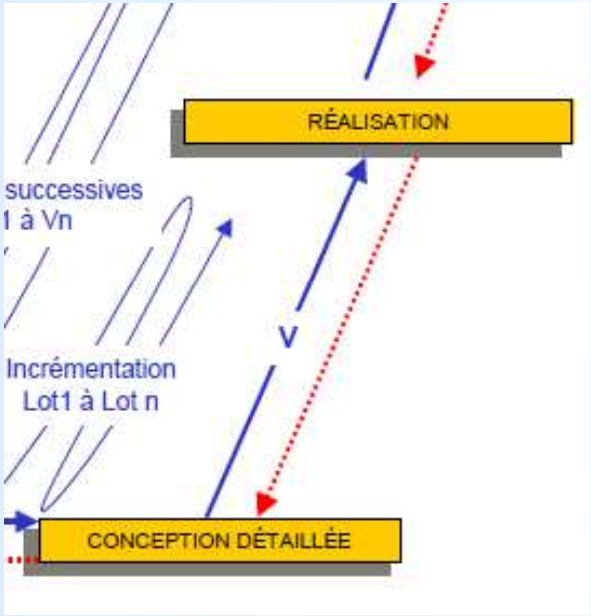
Étape 2 – Étude de faisabilité

L'étude de faisabilité vise à analyser la **faisabilité économique, organisationnelle et technique de projet**.
On s'interrogera notamment sur la faisabilité du projet en termes de produits éprouvés, rendement, ressources, compétences, capacité, financement et risques induits.
✓ *D'un point de vue SSI, il peut avoir été conclu lors de la phase précédente que cette phase ne devra pas comporter d'action SSI ; dans les autres cas, on affinera les éléments stratégiques, les contraintes juridiques, calendaires, financières.*

Étape 3 – Conception générale

Lors de la conception générale, on s'attachera à **affiner l'expression de besoins fonctionnels** sans rechercher les solutions techniques. On précisera également l'ensemble des contraintes et les différentes phase du projet.
*Soit on s'attache à rechercher les meilleurs pratiques SSI que devra mettre en oeuvre le SI considéré, soit on formalise le premier cahier des charges de sécurité sous la forme d'une fiche d'expression rationnelle des objectifs de sécurité (**FEROS**). Les objectifs de sécurité sont alors ajoutés au cahier des charges global du projet.*

Le projet



Étape 4 – Conception détaillée

À cette étape, la **maîtrise d'oeuvre est choisie**, le travail est donc réalisé conjointement maîtrise d'ouvrage et maîtrise d'oeuvre dans l'objectif de décrire finement l'engagement des deux parties en terme de réalisation. Cette étape permet d'aboutir au livrable appelé cahier des clauses techniques particulières (CCTP).

✓ *Dans le domaine de la SSI, seuls sont concernés les projets dont la prise en compte de la sécurité s'appuie sur une approche méthodologique. Pour ces projets, il s'agira de décrire des* ***solutions techniques et organisationnelles*** *qui sont retenues pour satisfaire les objectifs de sécurité formulés au sein du cahier des charges. Un tableau de bord SSI élaboré à partir des objectifs de sécurité pourra également être constitué.*

Étape 5 – Réalisation

La phase de réalisation comprend la réalisation des composantes du système d'information, c'est à dire le développement, l'intégration, la qualification et la recette.

Les phases de **développement, intégration et qualification** sont de la responsabilité du maître d'oeuvre, sous contrôle du maître d'ouvrage. En revanche, la recette qui est la vérification de la conformité du projet par rapport à la demande formulée dans le dossier validé de conception générale, est du ressort de la maîtrise d'ouvrage.

✓ *Pour la SSI, dans les projets qui le requièrent, cette étape permet au maître d'oeuvre de constituer la cible de sécurité, c'est à dire d'affiner les exigences de sécurité et* ***d'expliciter la façon dont ces exigences doivent être mises en oeuvre****.*

L’après projet

Étape 6 – Exploitation

Cette étape comprend **l'homologation** du système d'information, son déploiement, sa mise en oeuvre en situation opérationnelle, sa **maintenance** jusqu'à sa fin de vie.

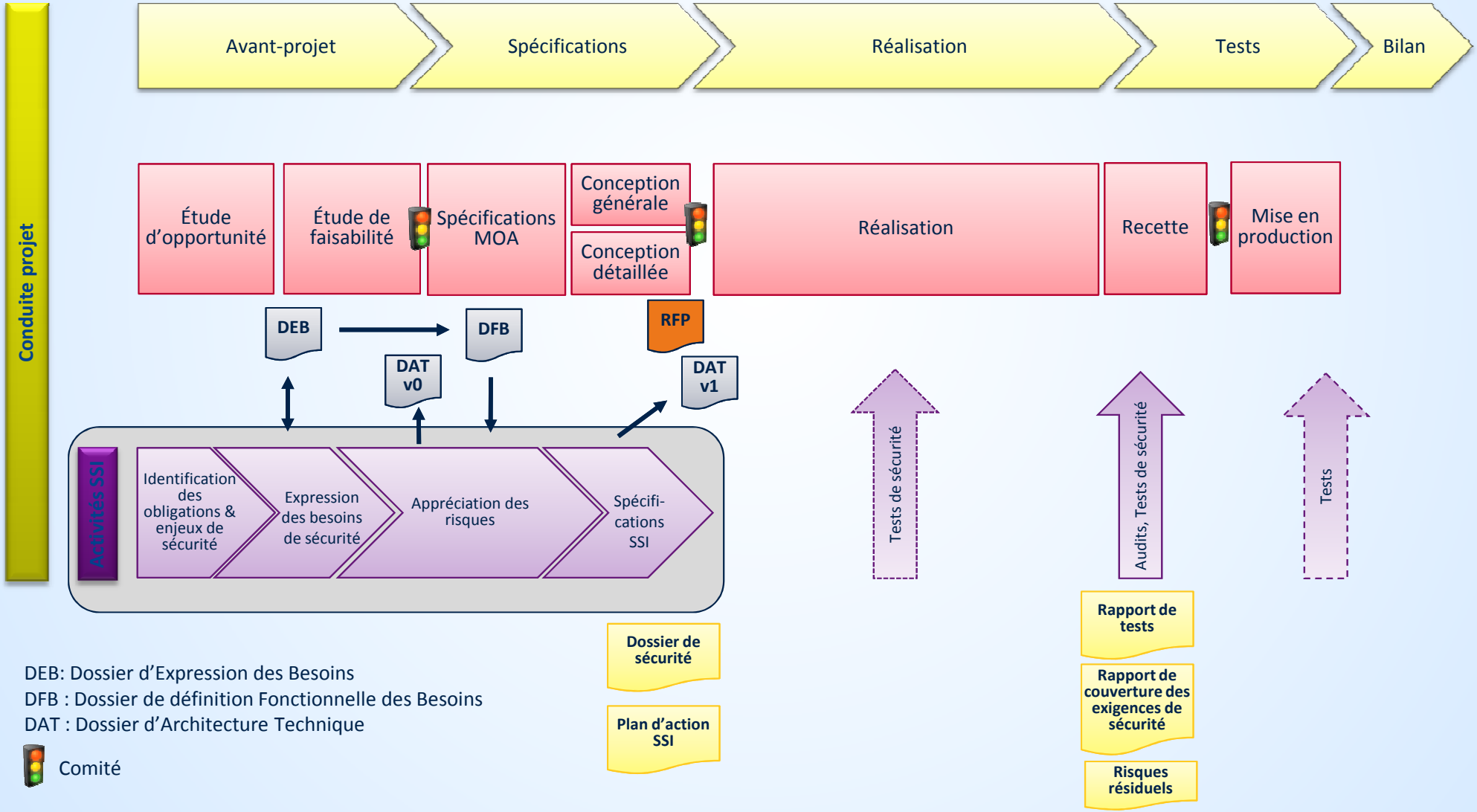
✓*Dans le domaine de la SSI, cette étape permet d'homologuer le système suite à un audit de sécurité vérifiant le* ***niveau de risque résiduel*** *et à la vue du dossier de sécurité du système. Ce dossier sera constitué de plus ou moins d'éléments en fonction des enjeux de sécurité. Par ailleurs, durant la phase d'exploitation, pour des systèmes requérant un haut niveau de maturité SSI, les différents intervenants alimenteront des tableaux de bord SSI dont les indicateurs sont issus des objectifs de sécurité du système.*

- Acceptation du projet par le « demandeur »
- Build2Run : transfert de responsabilités des équipes projet aux équipes RUN pour garantir le bon fonctionnement au jour le jour du « projet »

Pourquoi faire de la sécurité dans un projet ?

- Bonnes pratiques / règlementations ;
- Ne pas « détricoter » une solution parce qu'on n'a pas « anticipé » ;
- Le niveau de sécurité est adapté aux enjeux projet (ie gestion du risque);
- Impliquer l'ensemble des parties prenantes, de la définition des besoins sécurité à la mise en place de solutions adéquates (c'est l'affaire de tous!!)
- Références :
  - ❖ Guide d'intégration de la sécurité des systèmes d'information dans les projets (GISSP) de la DCSSI ;
  - ❖ OpenSAMM de l'OWASP ;
  - ❖ Microsoft Security Development Lifecycle (MSDL) ;

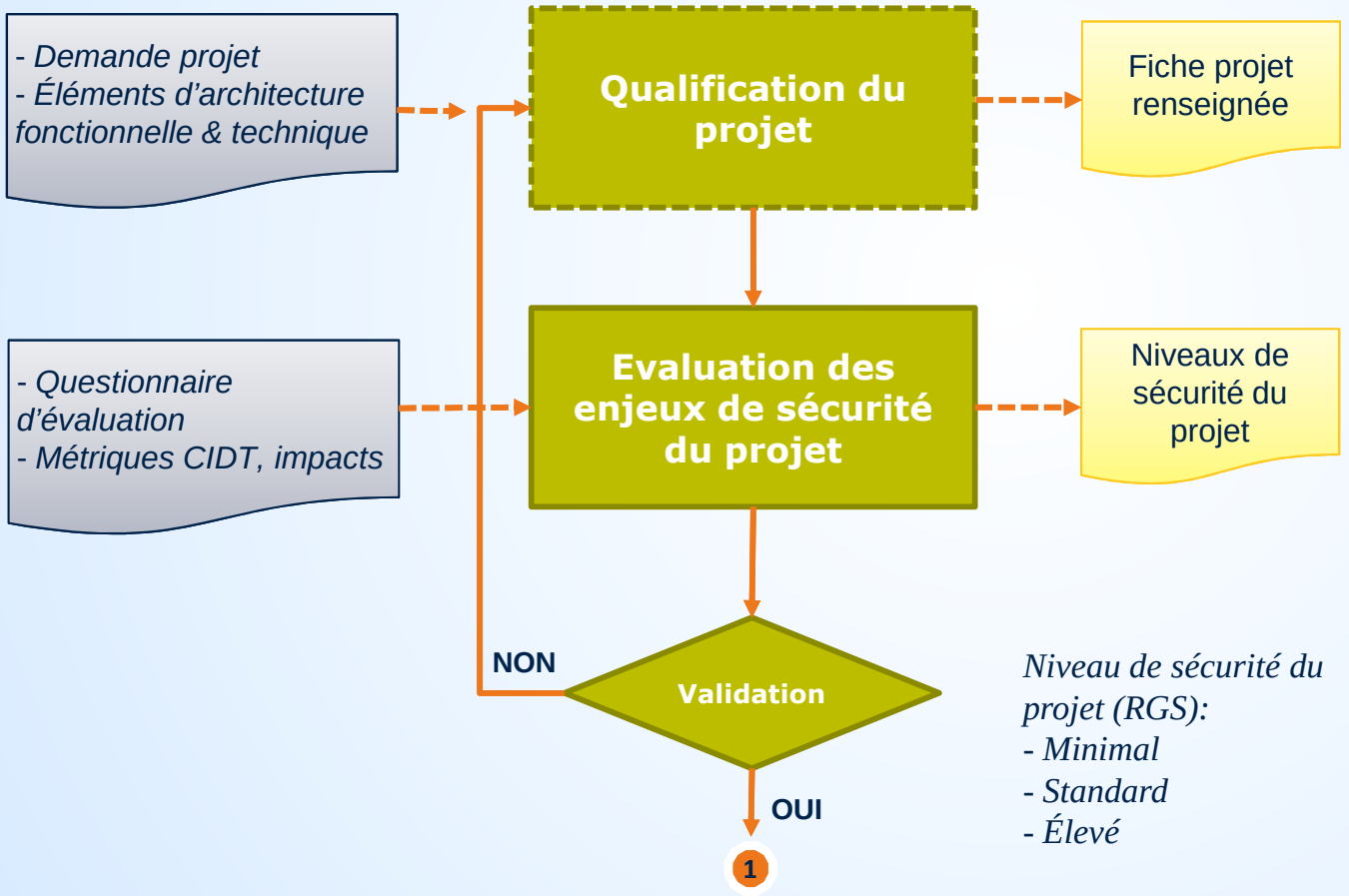
Démarche d'intégration de la SSI dans un projet



DEB: Dossier d'Expression des Besoins
DFB : Dossier de définition Fonctionnelle des Besoins
DAT : Dossier d'Architecture Technique

Comité

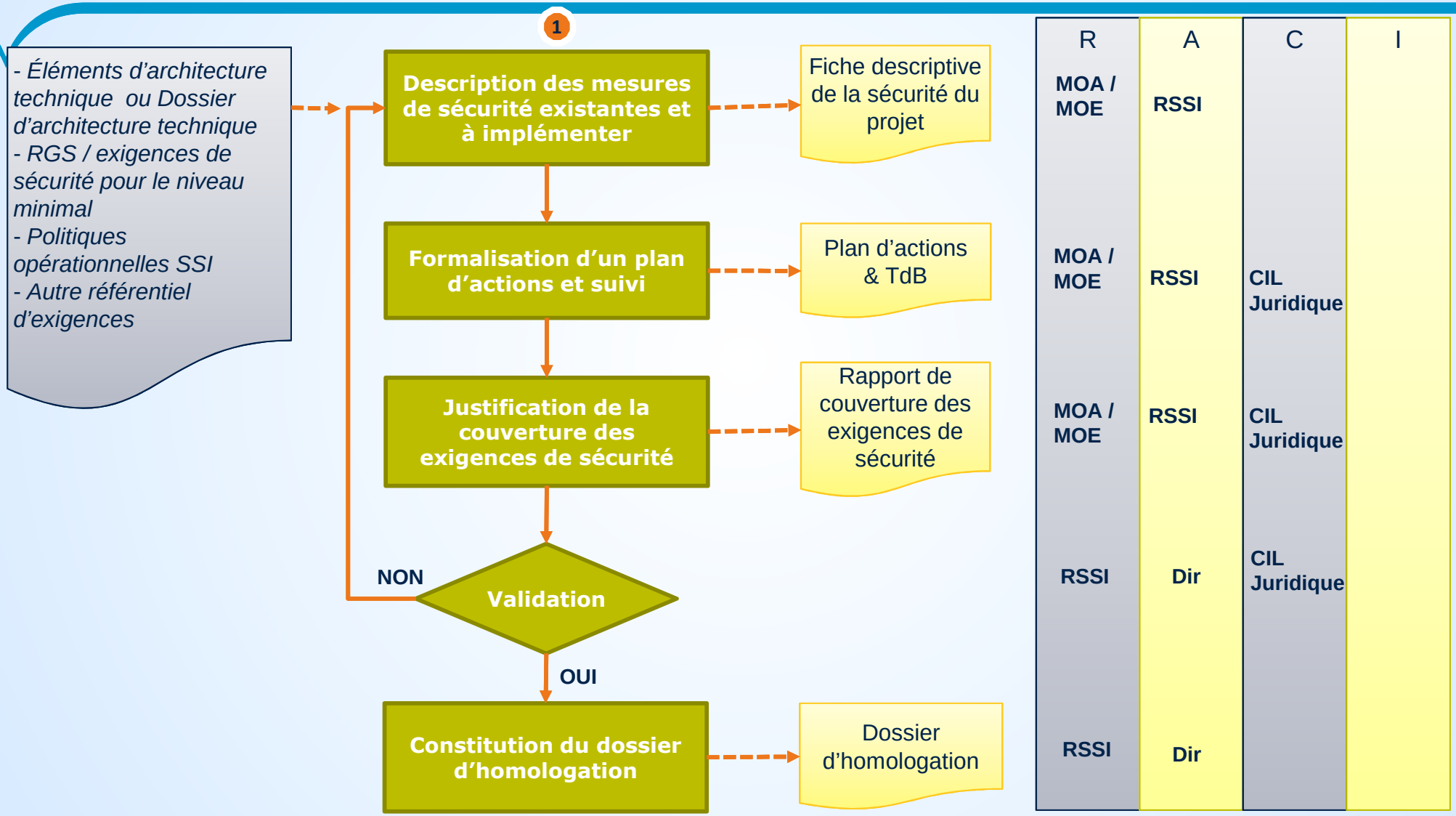
Qualification du niveau de sécurité



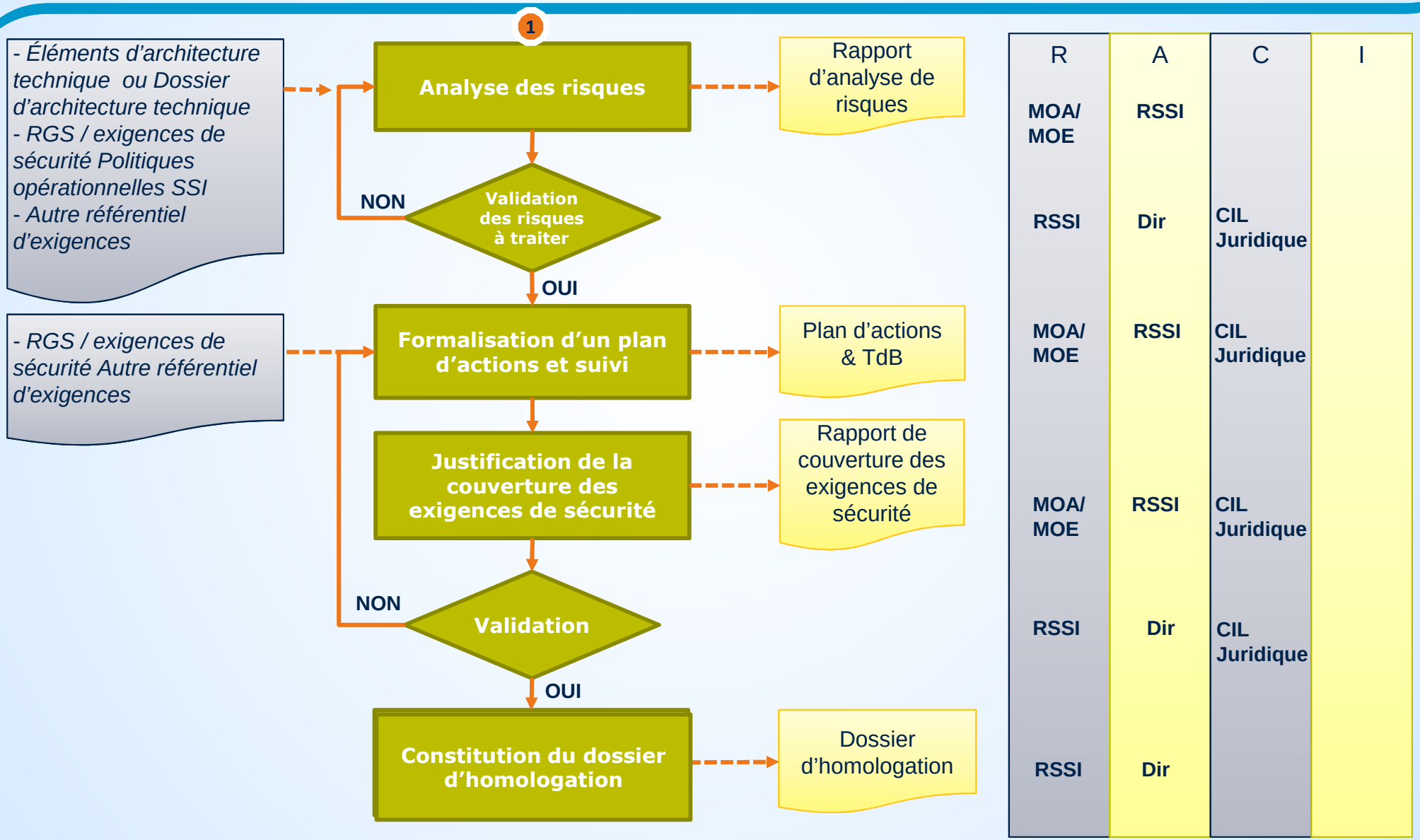
R	A	C	I
	MOA		
MOA	MOA	RSSI CIL	
RSSI	MOA	CIL Juridique	

R : Responsable de l'exécution de l'activité ;
A : Approuve les résultats de l'activité ;
C : Contribue à l'activité à titre consultatif ;
I : est Informé des résultats de l'activité.

Démarche simplifiée



Démarche standard



About Capgemini and Sogeti

With almost 140,000 people in over 40 countries, Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. The Group reported 2013 global revenues of EUR 10.1 billion. Together with its clients, Capgemini creates and delivers business and technology solutions that fit their needs and drive the results they want. A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™ and draws on Rightshore®, its worldwide delivery model.

Sogeti is a leading provider of technology and software testing, specializing in Application, Infrastructure and Engineering Services. Sogeti offers cutting-edge solutions around Testing, Business Intelligence & Analytics, Mobile, Cloud and Cyber Security. Sogeti brings together more than 20,000 professionals in 15 countries and has a strong local presence in over 100 locations in Europe, USA and India. Sogeti is a wholly-owned subsidiary of Cap Gemini S.A., listed on the Paris Stock Exchange.

Capgemini and Sogeti are experts in IT infrastructure and application integration. Together, we offer a complete range of cybersecurity services to guide and secure the digital transformation of companies and administrations. Our 2,500 professional employees support you in defining and implementing your cybersecurity strategies. We protect your data, IT and industrial systems, and the Internet of Things (IoT). We have the resources to strengthen your defenses, optimize your investments and control your risks. They include our security experts (Infrastructures, Applications, Endpoints, Identity and Access Management), and our R&D team that specializes in malware analysis and forensics. We have ethical hackers, five security operation centers (SOC) around the world, a licensed Information Technology Security Evaluation Facility, and are a global leader in the field of testing.

www.capgemini.com/cybersecurity
www.sogeti.com/cybersecurity