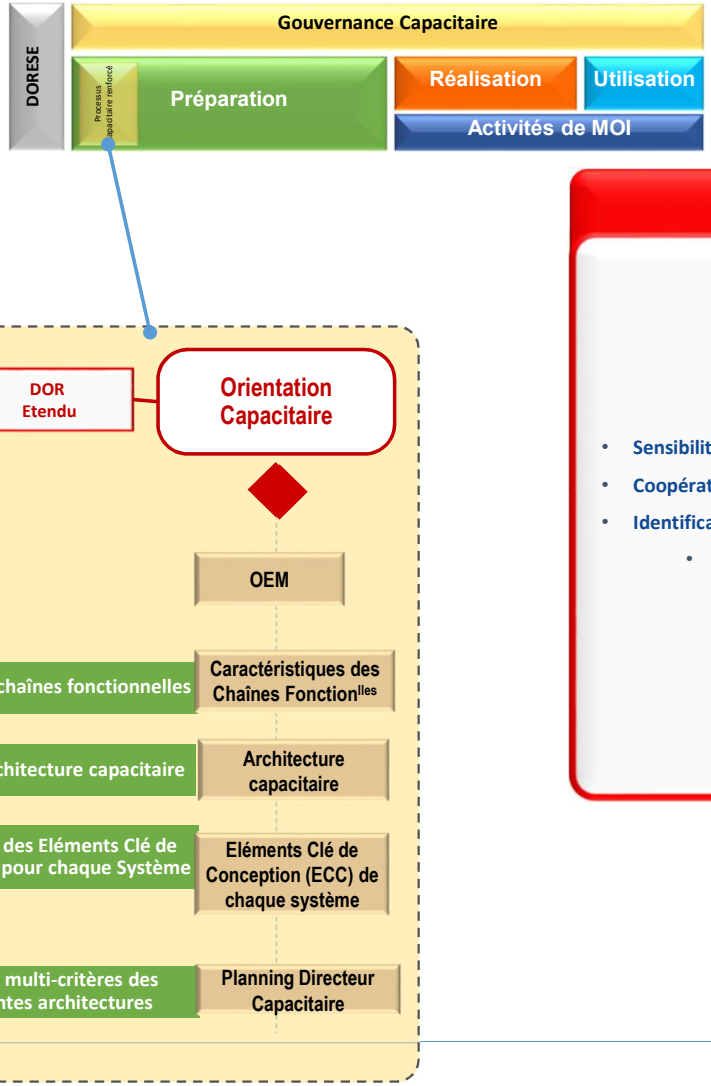
Calque 1618 – activités cyber

Les planches suivantes présentent les activités CYBER à mener étape par étape, tout au long du déroulement d'une opération (cadres rouges « activités cyber »)

Référence : 2022\CYBER\2\NP

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

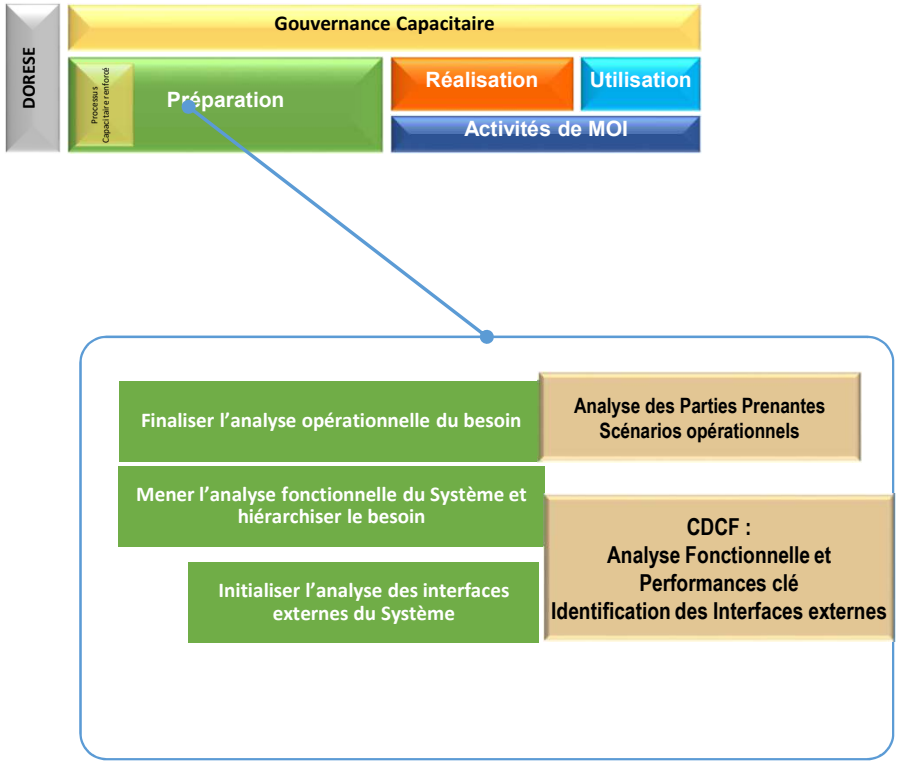
PROCESSUS CAPACITAIRE RENFORCE



ACTIVITES CYBER

- Sensibilité du sujet étudié
- Coopérations / parties prenantes
- Identification d'un «Cyber Officer » de l'opération dans chaque organisation
  - Mesures de sécurité à mettre en place avant le lancement (habilitations, réseaux, …)

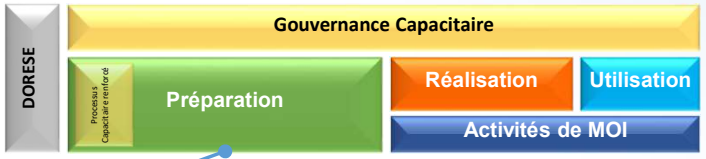
Consolidation de l'expression du besoin



ACTIVITES CYBER

- Expression des besoins de sécurité
  - Caractérisation macroscopique de la menace
  - Identification des biens essentiels à protéger
  - Evènements redoutés
- Prise en compte des besoins de sécurité dans les scénarios opérationnels
  - Typologie des acteurs
- Besoins d'exportabilité du système
- Patrimoine à protéger
- Analyse de l'impact sur la sécurité lié à l'interconnexion des systèmes en interface, identification du caractère multiniveau ou pas de ces interconnexions

Description des solutions d'architecture



Rechercher et décrire les options d'architectures de solution (y/c les systèmes contributeurs)

Description des options de solution (y/c soutien) Modélisations d'architecture

Liste des systèmes contributeurs (Infrastructures, qualification, etc)

Comparer / optimiser les options d'architecture de solution Mettre à jour les descriptions pour le DSP Choix (si nécessaire)

Proposition de choix

- Liste des solutions étudiées, performances, fourchette coûts associés, et tenue des ECC
- Matrice de choix multi-critères
- Analyse de la valeur
- Planning Directeur de l'OA

Préparer la comparaison des options d'architecture

Critères d'évaluation. Liste des études complémentaires à mener

Mener les études de comparaison des architectures de solutions (simulations, Démonstrateurs)

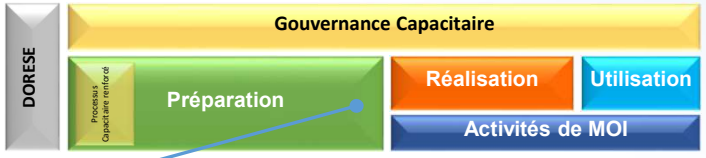
Evaluation des performances (dont coût)

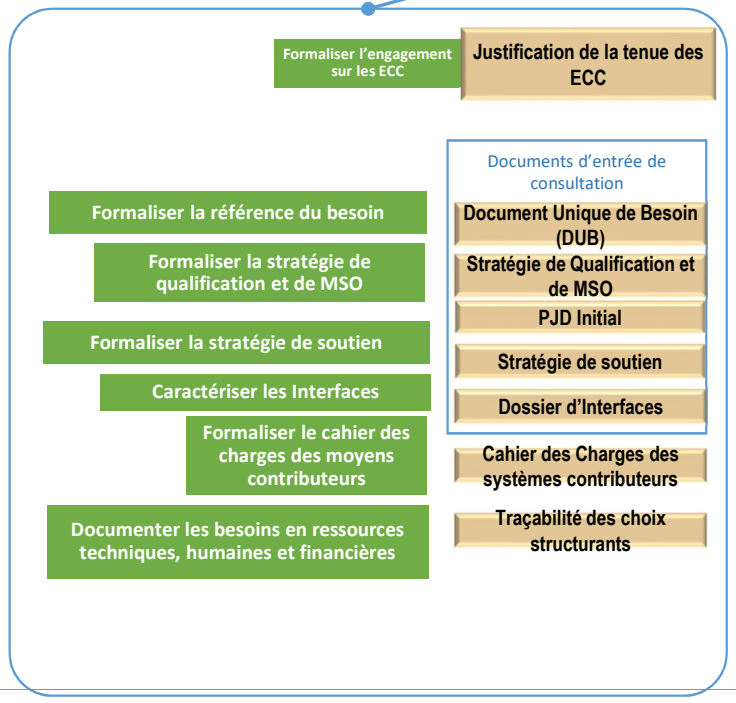
Contrats d'étude possibles

ACTIVITES CYBER

- Architecture technique préliminaire
  - Traduction des contraintes d'exportabilité (hardware commun?)
  - Règles de construction (simplification / clarification des architectures)
- Analyse de risques préliminaire
- Coopération (y compris chaîne de soutien)
- Sécurisation des environnements de réalisation (projet spécifique) => infrastructures, hommes, organisation, passerelles d'échanges, locaux,…
- Mise en place d'un GT « cyber » et une gouvernance appropriée sur le projet (mise en place de la commission de revue de la menace cyber).

Organisation de la phase de réalisation

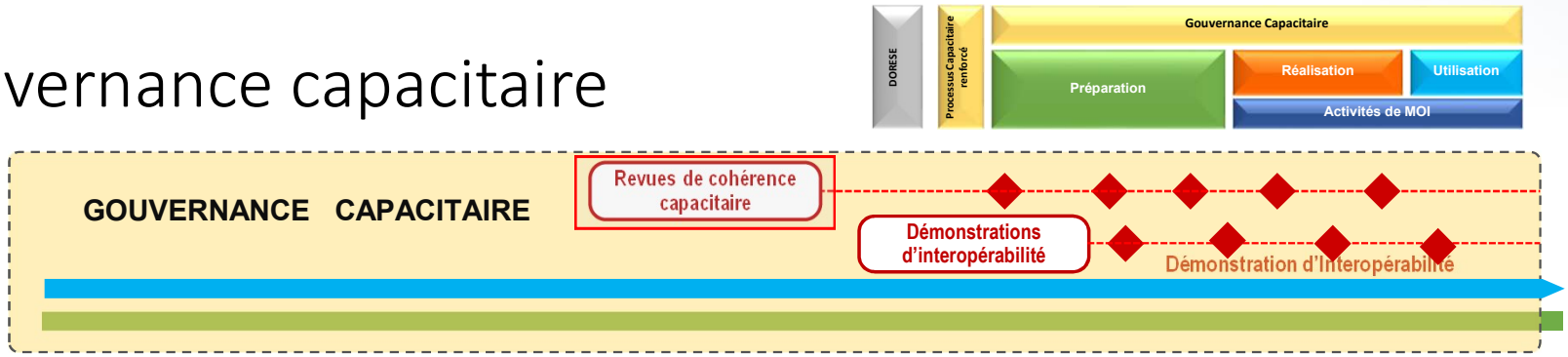




ACTIVITES CYBER

- Rappel ~~des Besoins en sécurité de la performance cyber attendue~~
- Objectifs de sécurité techniques
- Objectifs de sécurité organisationnels
  - Hypothèses d'utilisation du système
  - Scénarios, environnement,
- Annexe de sécurité
  - Obligations des parties prenantes en terme de sécurité
  - Plan de mise en place de des environnements sécurisés
- Liste des livrables/entrées étatiques attendus sur le domaine cyber
- Attendus pour franchissement des jalons
- Organisation du MCS / Stratégie de soutien doit intégrer un volet cyber et MCS
- Plan de management dérivant notamment l'organisation de la gouvernance cyber
- Planification globale des activités cyber y compris de la phase de remontée du V
- Processus d'homologation du système et des moyens d'essais à planifier
- Premier passage devant le collège multiniveau pour converger sur les mesures à appliquer
- Stratégie d'homologation à établir (intégrant le processus de maintien en condition d'homologation)

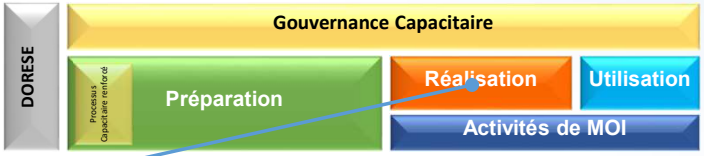
Gouvernance capacitaire



ACTIVITES CYBER

- Volet environnement sécurisé à la main de SSDI
- Volet produit à la main du comcyber et de la DGA (vision présentée en commission d'homologation)
  - Consolidation des dossiers de vulnérabilité au niveau supérieur
  - Analyse d'impact des évènements cyber de niveau système sur l'homologation de la capacité
  - Veille sur la menace (à décliner vers les systèmes via les commissions de revue de la menace cyber)
  - Maintien des activités MCS dont surveillance des systèmes

Phase de réalisation : descente du V



Montée en puissance des équipes et de la collaboration avec l'industrie

Assurer la mise à jour du besoin (intégration d'innovations – démarche agile)

Assurer la cohérence des interfaces avec les autres opérations d'armement
Assurer la gestion de configuration vis-à-vis des opérations en interface

Cycle de développement et de production industriel

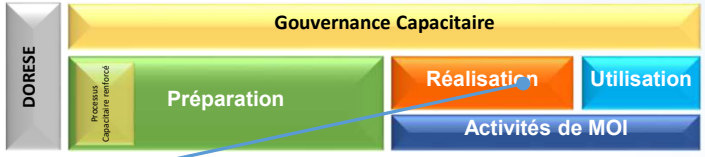
RSS, RCP, RCD, ...

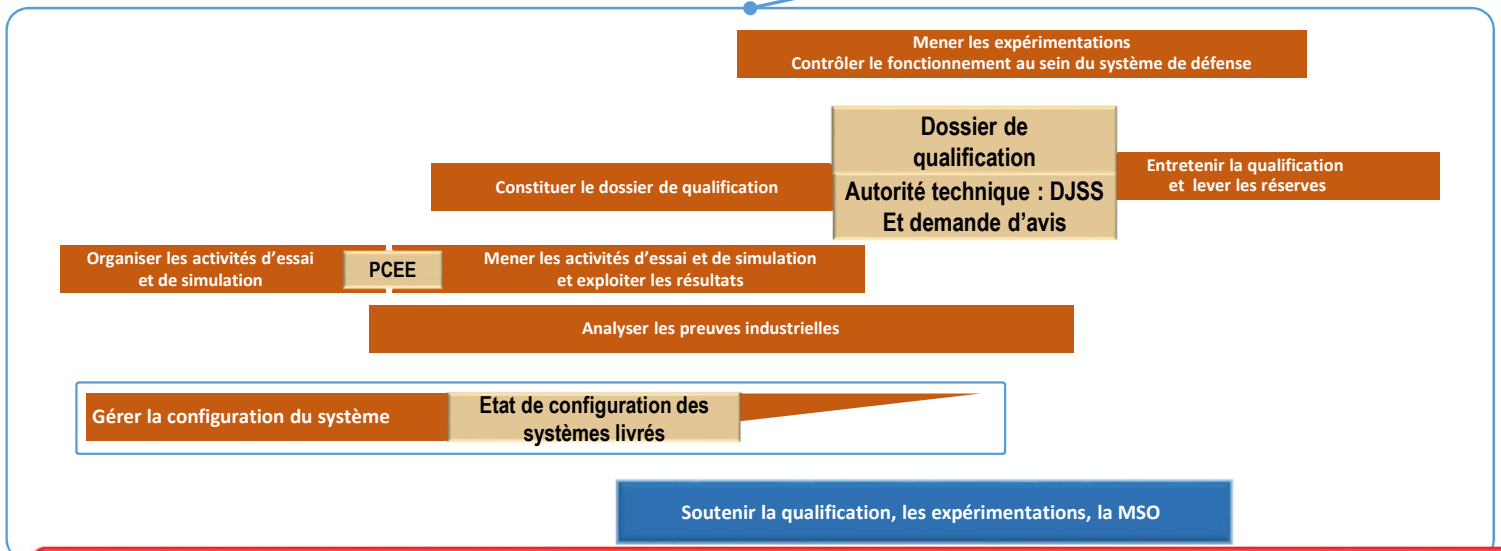
Concevoir et développer le système (incrément initial)

ACTIVITES CYBER

- Accompagnement (et non co-conception) en mode « agile » au fil de l'eau
  - Permet de faire progresser la maturité des sujets au fur et à mesure de l'avancée de la conception
  - Nécessite une véritable implication des opérationnels spécialistes de la cyber
- Jalons « grandes revues » permettant de cranter les choses à certains moments clés
  - Importance des critères de passages des jalons
  - Accord des parties prenantes sur le niveau de maturité attendue aux différents jalons
- Harmonisation des attendus des différentes revues entre industriels est moins essentielle (RCP, RCD, aptitude aux essais…)
- Importance de l'implication des opérationnels et des exploitants dans la démarche
- Gouvernance « cyber » à décliner dans la gouvernance globale des projets avec une vision supérieure à celle du projet
  - Prendre en compte l'aspect exportation également parmi l'ensemble des contraintes
  - Transparence, traçabilité
- Informer le bureau d'experts qui va instruire l'homologation du système + AH
- Informer le collège multiniveau restreint
- Volet formation / conduite du changement à prendre en compte
- Mise en place d'un GT « Cyber » est essentielle
  - mandat à définir / Compétences à identifier
- Application du processus de préparation de l'homologation
- Planification des activités cyber à entretenir

Remontée du V



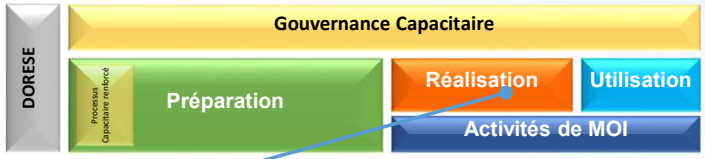


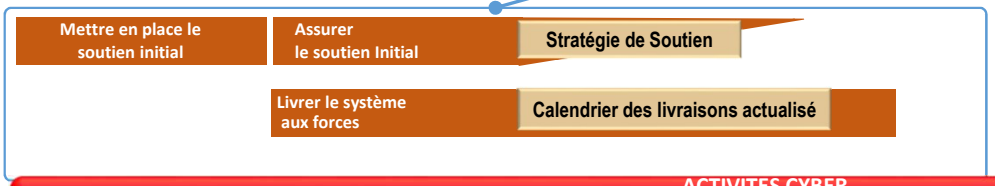
ACTIVITES CYBER

- Homologations provisoire à décliner selon les phases de vie du système, à prendre en compte pour les phases de de remontée du V, y compris pour les moyens d'essais. (Dossier de sécurité à constituer, Analyse de vulnérabilité à mener, audits)
- Second passage devant le collège multiniveau pour faire le bilan du niveau de sécurité atteint sur les interconnexions pour alimenter la commission d'homologation
- Evaluations du système lui-même mais aussi du système dans les chaînes fonctionnelles globales, y compris impact des mesures « cyber » sur les performances globales des autres chaines fonctionnelles
  - La représentativité du produit testé vis-à-vis du système final à prendre en compte
  - Planification de tests type Pentests, tests « libres », test de continuité d'activités ou de reprise sur incident, VAMOM orientée MCS
  - Scénarios de test à définir vis-à-vis des évènements redoutés
- Prise en compte de la réinsertion des mesures de sécurité sur le système, au fur et à mesure de son développement (en général débrayées en conception)
- Planification à maintenir (pb de coactivités)

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

Mise en place du soutien



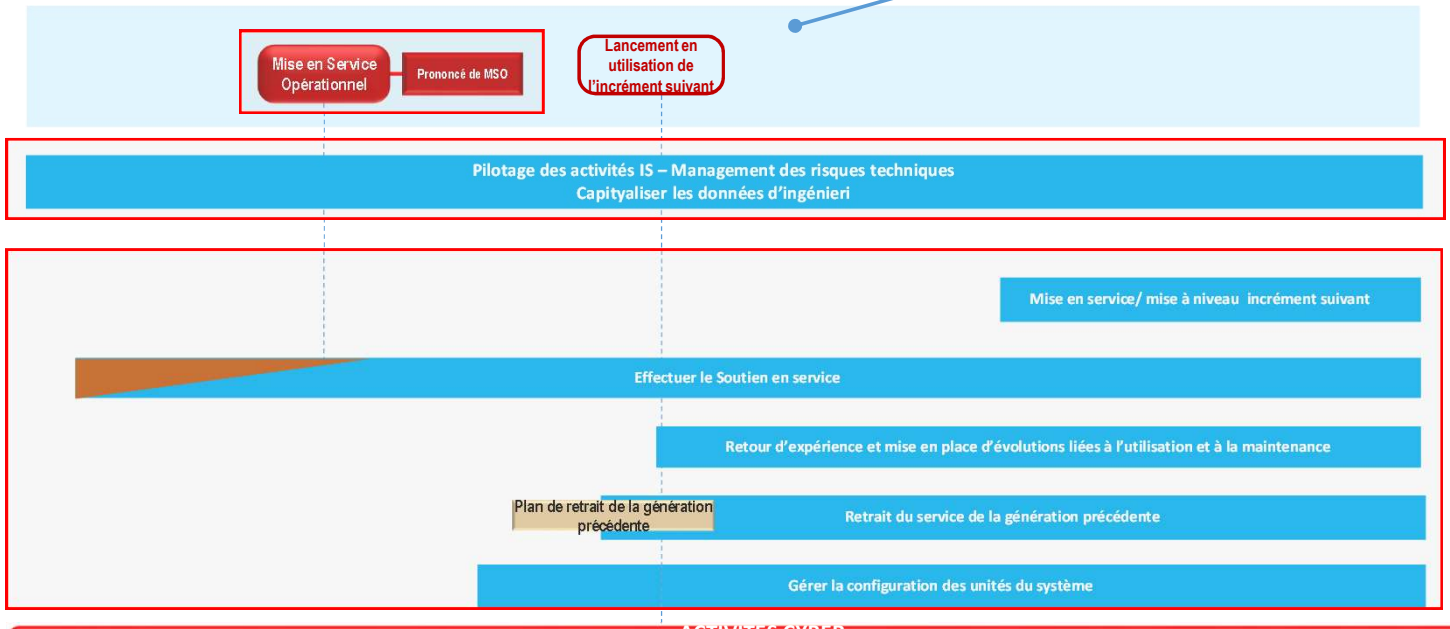


ACTIVITES CYBER

Maintien en condition d'homologation dont MCS :

- Principes à établir très en amont car peut influer sur l'architecture du système et sur l'organisation
- Application du processus de maintien en condition d'homologation
- Stratégie de mise à jour des systèmes vis-à-vis de leur vulnérabilité, en regard des process de V&V qui méritent d'être plus ou moins repris.
- Temps relatifs de réalisation des systèmes très différent du temps des évolutions « cyber » ou des menaces à prendre en compte (il existe déjà de nouvelles vulnérabilités pour un système alors qu'il est tout juste livré) => se mettre d'accord à l'avance sur la fréquence des analyses / mises à jour des différentes parties du système
- Veille technique à mettre en place sur des objets parfois non classiques, donc peu documentée. Les échanges d'informations entre les différents acteurs (étatiques, industriels) sont nécessaires. Il faut mettre en place une organisation adaptée à la veille. Plan MCS à définir, probablement dès le début de la réalisation.
- Dialogue nécessaire avec les opérationnels
- Interconnexion entre le processus de MCS et le processus de gestion de configuration globale à définir pour conserver la rigueur de l'approche globale de la gestion de configuration (préserver la performance globale, dont safety). Procédures d'urgence à mettre en place éventuellement. Le partage de la connaissance des configurations appliquées est encore plus important dans un contexte de vulnérabilité Cyber.
- Logique d'enrôlement des systèmes au fur et à mesure de leur production à établir
- Logistique à mettre en place sur la récupération et l'analyse des logs. Logistique à mettre en place sur l'analyse après incident.

Phase d'utilisation



ACTIVITES CYBER

Importance du retour d'expérience à faire remonter vers l'industrie.

Importance de l'articulation entre la garantie, le MCO, la complétude des essais qui ont permis de sanctionner la réception des phases de production

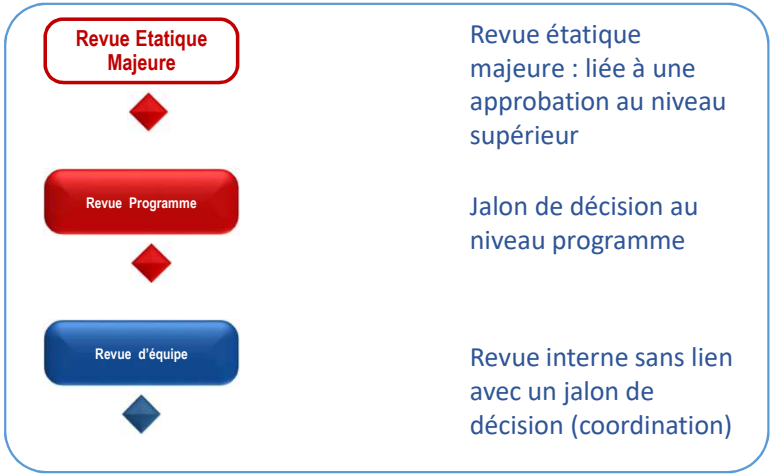
Application du processus de maintien en condition d'homologation

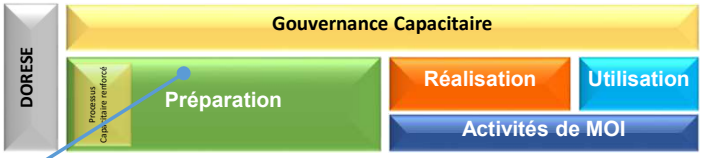
Importance de la gestion de conf au sens enregistrement, mais aussi gouvernance sur la décision de prise en compte des demandes d'évolution et de changements. Analyses de risques à produire pour instruire les demandes de changements (est-ce que cette analyse de risque est un article de configuration spécifique)

Analyse vulnérabilité et audits, à programmer pour maintien de l'homologation du système

Prise en compte de la cyber lors des revues

Jalonnement des opérations : principales revues





Revue d'ingénierie de cadrage

Revue d'ingénierie de cadrage

ENJEUX

S'assurer de la complétude de l'analyse du besoin
Etre dans les conditions de lancer le travail de comparaison des solutions d'architecture

OBJECTIFS

ACTEURS

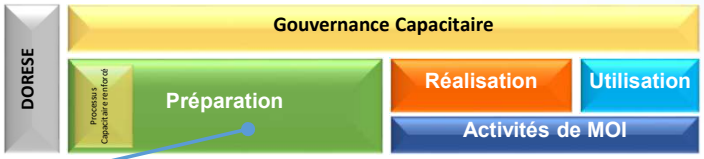
DONNEES D'ENTREE

SORTIES

Evaluation de la charge d'analyse globale numérique, (pas forcément que les experts Cyber), liée à l'évaluation de la résilience des systèmes à concevoir (maitrise d'oeuvre de rang 0 indispensable en « cyber »)

Sur le fond, vérifier que la dimension « vulnérabilité cyber » est prise en compte dans les travaux qui vont permettre de choisir la bonne architecture (les travaux prévus doivent expliciter quel type d'études, par qui et quand)

Planifier la sollicitation des avis qui seront utiles pour se prononcer sur l'acceptabilité du système à terme.



Revue de dimensionnement technique

Revue de Dimensionnement Technique

ENJEUX

Vérifier la faisabilité technique et la soutenabilité RH de l'opération

OBJECTIFS

1. Evaluer la charge nécessaire en RH pour soutenir l'opération
2. Optimiser la stratégie d'ingénierie en fonction des ressources RH mobilisables

ACTEURS

DONNEES D'ENTREE

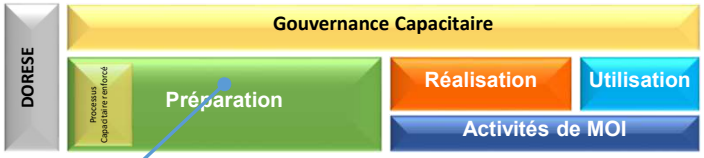
SORTIES

Evaluation de la charge d'analyse globale numérique, (pas forcément que les experts Cyber), liée à l'évaluation de la résilience des systèmes à concevoir (maitrise d'oeuvre de rang 0 indispensable en « cyber »)

Sur le fond, vérifier que la dimension « vulnérabilité cyber » est prise en compte dans les travaux qui vont permettre de choisir la bonne architecture (les travaux prévus doivent expliciter quel type d'études, par qui et quand)

Planifier la sollicitation des avis qui seront utiles pour se prononcer sur l'acceptabilité du système à terme.

Définition des grands objectifs techniques transverses et de l'organisation mise en place pour la traiter au sein du groupe complet (DGA, industries, …) (rôles, responsabilité, précision des « domaines de confiance » à poser pour respecter les contraintes de l'environnement cyber)



Comité des devis

Comité des devis

ENJEUX

Valider le devis de l'opération

OBJECTIFS

ACTEURS

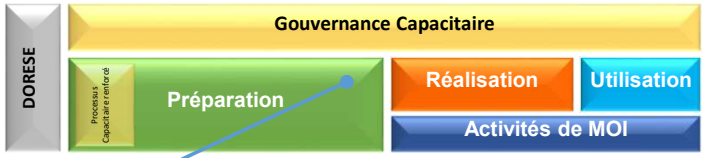
DONNEES D'ENTREE

Trade off à faire en AV doivent être faits en prenant en compte l'aspect cyber

Positionnement des marges pour aléas en fonction des risques cyber également / Robustesse vis-à-vis de l'évolutivité de la menace. (revisite périodique du devis vis-à-vis de la menace?)

Cohérence des attendus vis-à-vis des opérations connexes (équipements B, opérations en interface)

SORTIES



Revue de hiérarchisation des solutions

Revue d'ingénierie de hiérarchisation des solutions

ENJEUX

Être dans les conditions de pouvoir justifier un choix de solution
Pouvoir lancer la rédaction des éléments de consultation sur un choix de solution d'architecture validé

OBJECTIFS

ACTEURS

DONNEES D'ENTREE

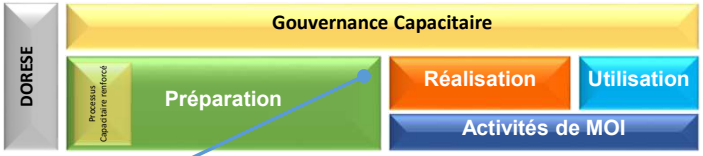
Bilan de l'évaluation de la performance cyber des différentes solutions envisagées

ECC « cyber » caractérisés et évalués

Choix « système » à faire au vu des analyses de sécurité effectuées sur les systèmes eux-mêmes, mais en prenant en compte également les analyses de sécurité faites au niveau capacitaire.

La revue présente la synthèse des travaux d'architecture menés sur toute la phase précédente, en faisant le lien entre la vision capacitaire et la vision système (vrai rôle de grand architecte lié au rôle de maitre d'œuvre de rang 0)

SORTIES



Revue de lancement de la consultation

Lancement de la Consultation

ENJEUX

Valider la cohérence et la complétude du corpus documentaire de consultation

OBJECTIFS

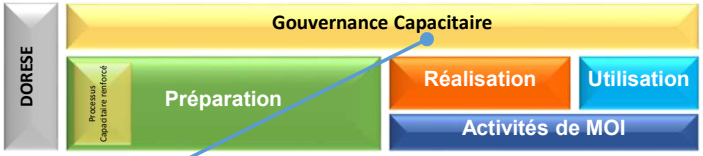
ACTEURS

DONNEES D'ENTREE

Préparation des éléments liés à la sécurité des échanges à mener pdt la consultation : type annexe de sécurité, ciblée pour la partie consultation, mais également qui permet aux industriels de se projeter sur le coût de la protection du secret liée au marché, pour sa phase d'exécution.

Point sur le référentiel applicable

SORTIES



Revue de cohérence capacitaire

Revues de Cohérence Capacitaire

ENJEUX

Garantir que l'objectif capacitaire est convenablement pris en compte par les différentes opérations d'armement contribuant à cet objectif. Vision calendaire et impacts des choix ou aléas.

Fréquence des revues à évaluer (semestriellement?)

OBJECTIFS

- Analyser de façon récursive les évolutions d'architectures et l'impact sur la performance cyber de niveau capacitaire (contexte très évolutif pour ce qui concerne les menaces, les techno, mais également les feuilles de route des systèmes avec leurs aléas potentiels)
- Analyse d'impact des activités d'homologation de niveau système sur l'homologation de la capacité
- Prendre en compte la totalité des systèmes concourant au déroulement d'une mission opérationnelle (ex Pmis + Système avion + Chiffrement + moyens de comm, …) pour évaluer la vulnérabilité.
- Attention à bien réévaluer la vision globale en fonction des réelles possibilités techniques applicables par les différentes briques
- Trouver le meilleur compromis sur ce qui est faisable du point de vue économique global.

ACTEURS

Participation systématique du chargé de mission cyber

Nécessité de compétence de niveau maitrise d'œuvre de rang 0, permettant de cadrer les bon niveaux d'engagement vis-à-vis des industriels

SORTIES

Identification des risques et plans d'action associés

Portefeuille d'actions à suivre.

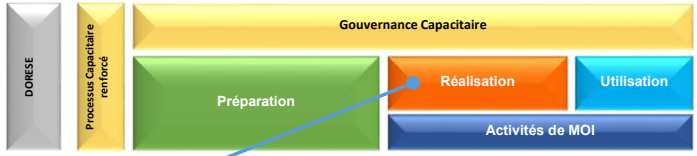
DONNEES D'ENTREE

ECC de niveau Cyber

Vision calendaire de la mise à dispo des différentes composantes

Vision économique d'ensemble permettant de cadrer ce qui est faisable ou non

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité



Revue de synchronisation et de lancement

Réunion de synchronisation et de lancement

ENJEUX

Synchroniser les équipes sur la compréhension du périmètre technique et sur le calendrier de la phase

OBJECTIFS

- Réaffirmer l'importance du volet cyber dans ces réunions de lancement, avec mise en place de l'organisation avec réaffirmation du rôle des responsables sécurité côté industriel et étatique (« cyber officer », ou Product Cyber Security Authority », capable d'endosser les trade off qui seront nécessaires pdt la conception du système)
- 2 rôles à définir/organiser : le porteur de la sécurisation du programme, et le porteur de la performance cyber globale de niveau capacitaire

ACTEURS

DONNEES D'ENTREE

- Rappel des objectifs de performance du système et des ECC cyber

SORTIES

Revue d'aptitude aux essais

Revue d'aptitude aux essais

ENJEUX

Être prêt pour les essais de qualification étatique

OBJECTIFS

ACTEURS

Bien rappeler le niveau de confidentialité du résultat des essais y compris de ce qui peut être découvert sur les systèmes connexes

DONNEES D'ENTREE

- Homologation : Approval for testing qui autorise l'utilisation du système raccordé à d'autres moyens techniques homologués.
- Disponibilité des PES des systèmes concernées
- Disponibilité des moyens connexes
- Capacité à réinstaller le système en cas d'essais destructifs (complexité à évaluer au cas par cas)
- Programme d'essai partagé entre les acteurs
- Audit de configuration du système à évaluer (y compris documentation)
- Formation des personnes amenées à manipuler le système
- Résultats d'un premier lot d'essais prévus au PJD, permettant de justifier la maturité du système.

SORTIES

Revue de qualification

Revue de qualification → Prononcé de Qualification

ENJEUX

Pouvoir émettre un avis sur la possibilité de prononcer la qualification, assorti de recommandations.

OBJECTIFS

- Vérifier que le système est prêt pour obtenir une autorisation provisoire d'emploi

ACTEURS

RSSI P sollicité sur les éventuelles dérogations, qui organise un arbitrage vis-à-vis de l'AH.

DONNEES D'ENTREE

- Preuves de conformité du système aux exigences cyber (dont PCI/PRI si besoin) et/ou vérification de la tenue des performances cyber
- .

SORTIES

- Recommandations ou demandes de modification
- Réserves éventuelles ou dérogations

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

Revue de Mise en service opérationnelle

Mise en Service Opérationnel — Prononcé de MSO

ENJEUX

S'assurer que les conditions sont requises pour utiliser le système dans un contexte opérationnel. (les axes DORESE sont tous couverts)

OBJECTIFS

ACTEURS

Transition entre RSSI P et RSSI A

Rôle des organismes de soutien dans le maintien de la vision cyber (gestion de conf, cartographie, audits de configuration)

DONNEES D'ENTREE

- Homologation ferme (résultats d'audit, analyse de vulnérabilité résiduelle)
- Résultats de tests type pentests, ou red team
- Entrainement « cyber » des équipes opérationnelles (PCI/PRI)
- Evaluation sur le plan capacitaire du comportement du système (performances, protection, résilience, surveillance …) qui peut donner lieu à des revues spécifiques (Vérification des Capacité Militaire) pour la marine
- Vérification de la prise en compte des contraintes cyber sur l'ensemble des acteurs du soutien (ensemble des partenaires) qui peuvent être différents au passage au stade d'utilisation
- Condition du maintien de l'homologation dans le temps (veille des menaces, gestion de la dette SSI et suivi du portefeuille des vulnérabilités)

SORTIES