Audit & contrôle

Contrôle de la Sécurité des S.I.

Démarche

3. Les démarches de contrôle

- La Planification des Contrôles
- Le Déroulement d'un Contrôle
  - Le Cadrage
  - Les Investigations
  - La Restitution
- Points clefs
  - *Cas concret : Banque en ligne*
  - *Cas concret : Réunion de lancement*
  - *Mise en pratique : cadrage et de planification d'un audit*

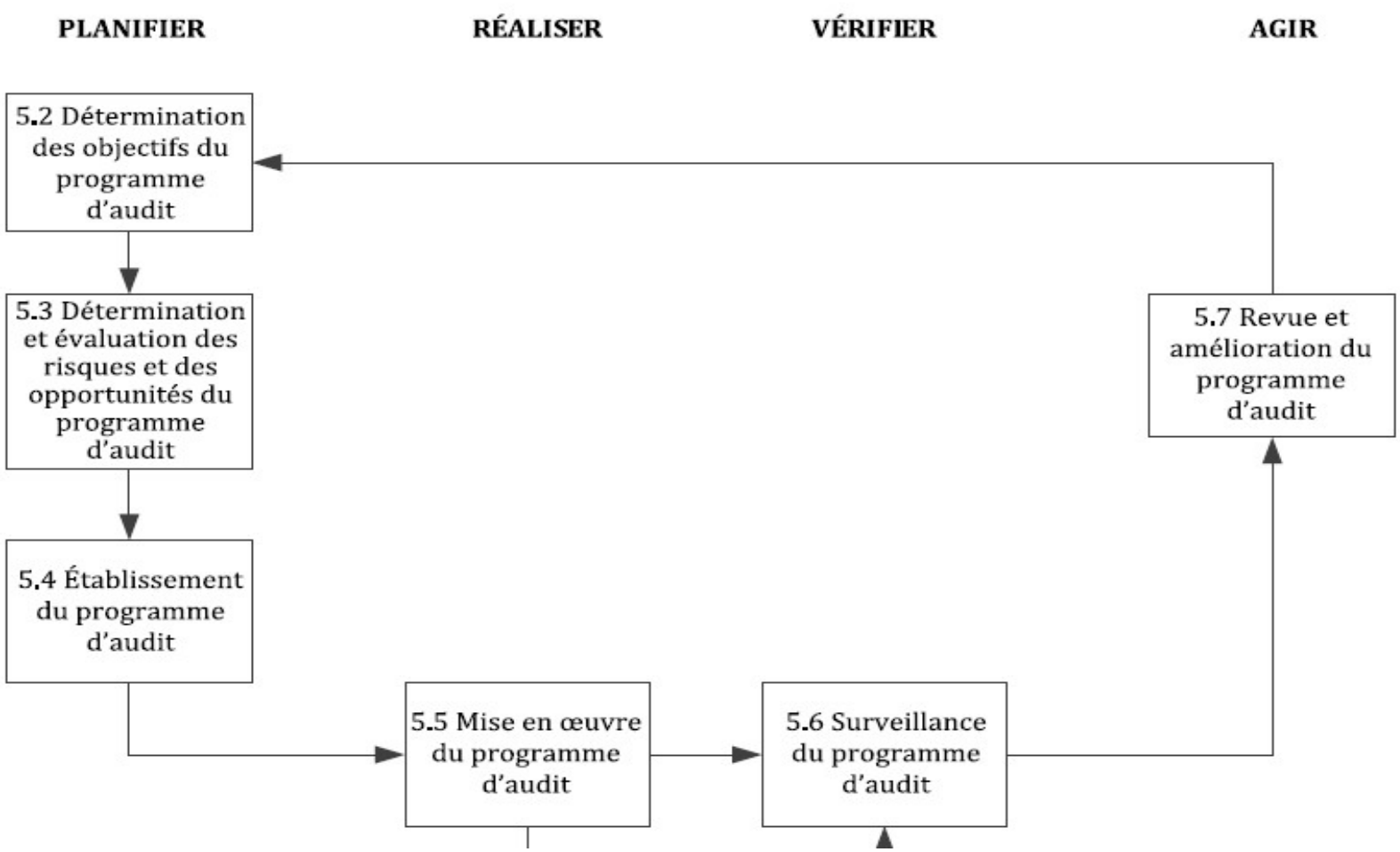
Planification : Le programme de contrôle

⇨ **L'activité de contrôle s'appuie sur une planification court et moyens termes des activités, explicitée au sein d'un plan de contrôle (annuel en général).**

⇨ **Le plan de contrôle précise l'ensemble des contrôles à mener, et indique pour chacun :**

- ✓ Le périmètre concerné
- ✓ Les risques concernés par les contrôles SSI
- ✓ Les actifs, processus, organisation, … objets des contrôles SSI
- ✓ La nature des investigations
- ✓ Le planning, fréquence, … des contrôles unitaire
- ✓ Les moyens nécessaires à réaliser les contrôles SSI

Planification : Le programme de contrôle



Planification : Le programme de contrôle

Dans un établissement bancaire, l'analyse de risque a mis en avant des risques de cyberattaque sur la banque en ligne (site bancaire sur internet)

⇨ **Planifier les contrôles à mener**

Planification : Le programme de contrôle

⇨**Démarche appliquée :**

- ✓ Identification des services de la Banque en Ligne et de leur niveau de sensibilité en matière de sécurité (DICT)
- ✓ Classification des services par bloc fonctionnel en fonction des critères de sécurité :
  - Besoin de sécurité DICT
  - Degré d'exposition du service
  - Implication d'acteurs externes
- ✓ Sélection des actifs à retenir et choix des investigations à lancer
- ✓ Planification des contrôles

Planification : Le programme de contrôle

⇨**Services retenus pour les contrôles :**

- ✓ Accès par le Canal Internet
  - Module « Opérations souscription et Virement »
  - Module « Bourse »
  - Module « Gestion de compte et Alertes»
- ✓ Accès par le Canal Internet Mobile
  - Modules « Passerelle Internet Mobile»
- ✓ Accès par le Canal Téléphonie
  - Module « Virement »
  - Module « Bourse »
  - Module « Gestion de compte et Alertes »
- ✓ Backoffice
  - Module « GA-BAD et CQ Publication Dynamique »

Planification : Le programme de contrôle

⇨Résultat :

	Nature des contrôles			2010		2011		2012	
	Applicatif	Infra	Process	S1	S2	S1	S2	S1	S2
Canal Internet									
Module « Opérations souscription et Virement »	X		X						
Module « Bourse »	X		X						
Module « Gestion de compte et Alerte »	X		X						
Canal Internet Mobile									
Module « Passerelle Internet Mobile»		X	X						
Canal Téléphonie									
Module « Virement »		X	X						
Module « Bourse »		X	X						
Module « Gestion de compte et Alerte»		X	X						
Backoffice									
Module « GA-BAD et CQ Publication Dynamique	X	X	X						

150 000 €	130 000 €	150 000 €

Planification : Le programme de contrôle

En synthèse :

Actifs Critiques + Risques

Périmètre à contrôler

Le déroulement d'un contrôle

La norme 19011 : objectif

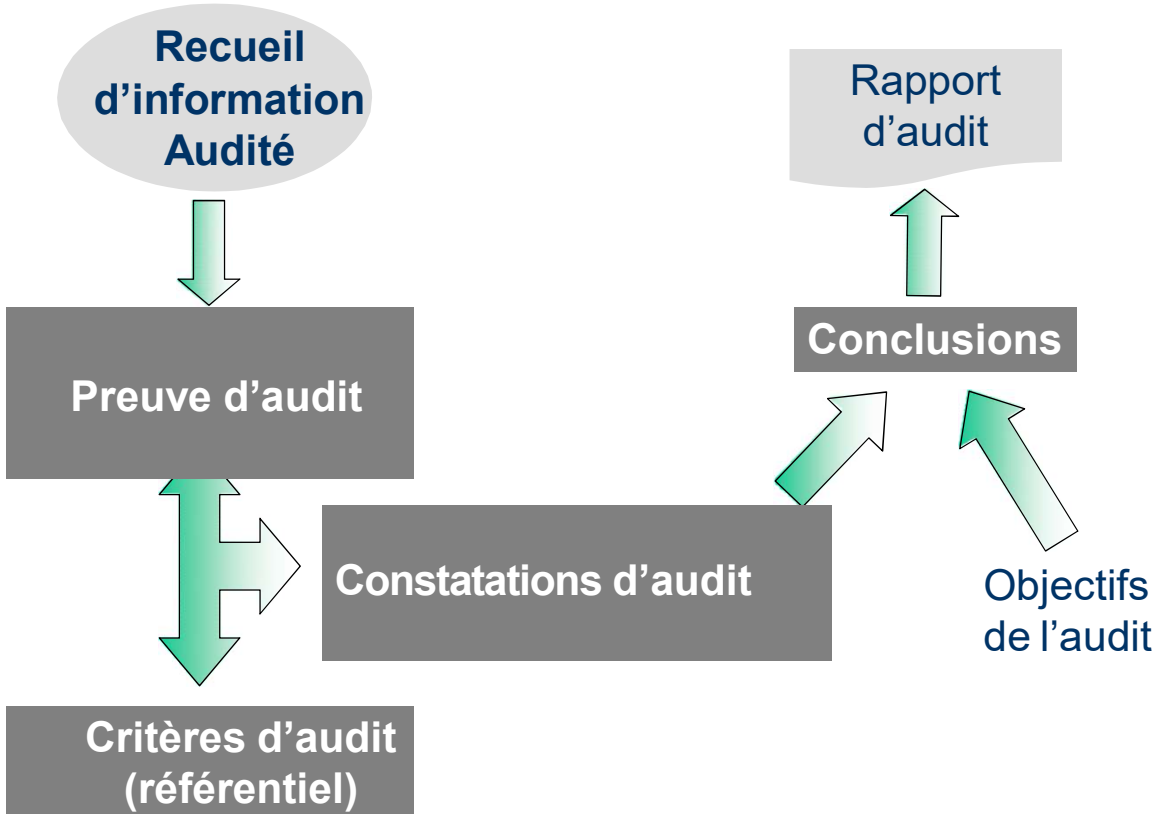
La présente Norme internationale fournit des lignes directrices sur l'audit de systèmes de management, comprenant les principes de l'audit, le management d'un programme d'audit et la réalisation d'audits de systèmes de management. Elle donne également des lignes directrices sur l'évaluation de la compétence des personnes impliquées dans le processus d'audit, y compris le ou la responsable du management du programme d'audit, les auditeurs et les équipes d'audit.
Elle est applicable à tous les organismes qui doivent réaliser des audits internes ou externes de systèmes de management ou manager un programme d'audit.
La présente Norme internationale peut, en principe, s'appliquer à d'autres types d'audits, à condition toutefois d'accorder une attention toute particulière aux compétences spécifiques requises.

Article 1

Domaine d'application

- Un guide de bonnes pratiques d'audit (« génériques »)
  - Pour les auditeurs
  - Pour les audités

Le déroulement d'un contrôle



117

Le déroulement d'un contrôle

Préparation

Avant

- Déclenchement de l'audit
- Préparation des activités d'audit sur site

Audit sur site

Pendant

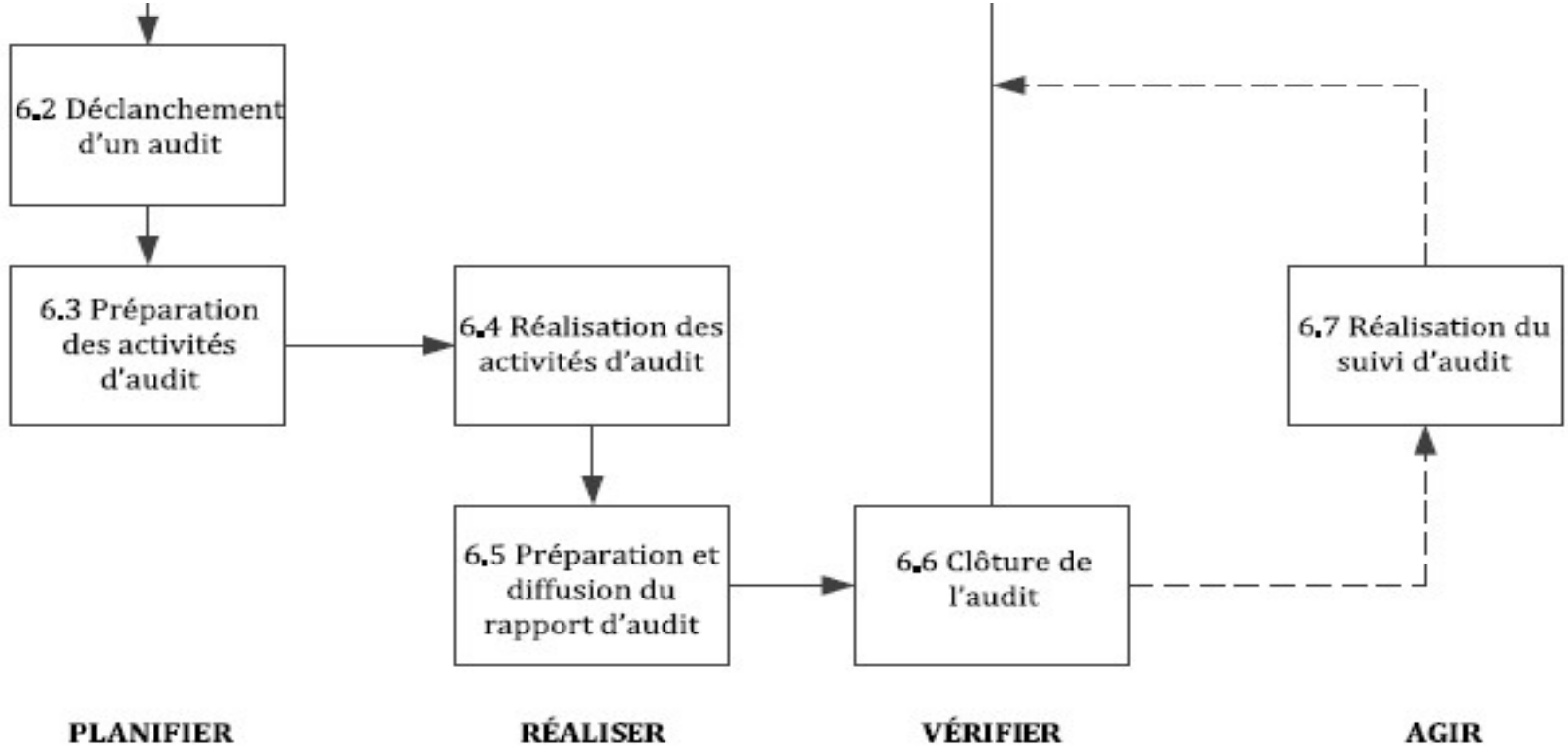
- Activités d'audit sur site

Clôture-suivi

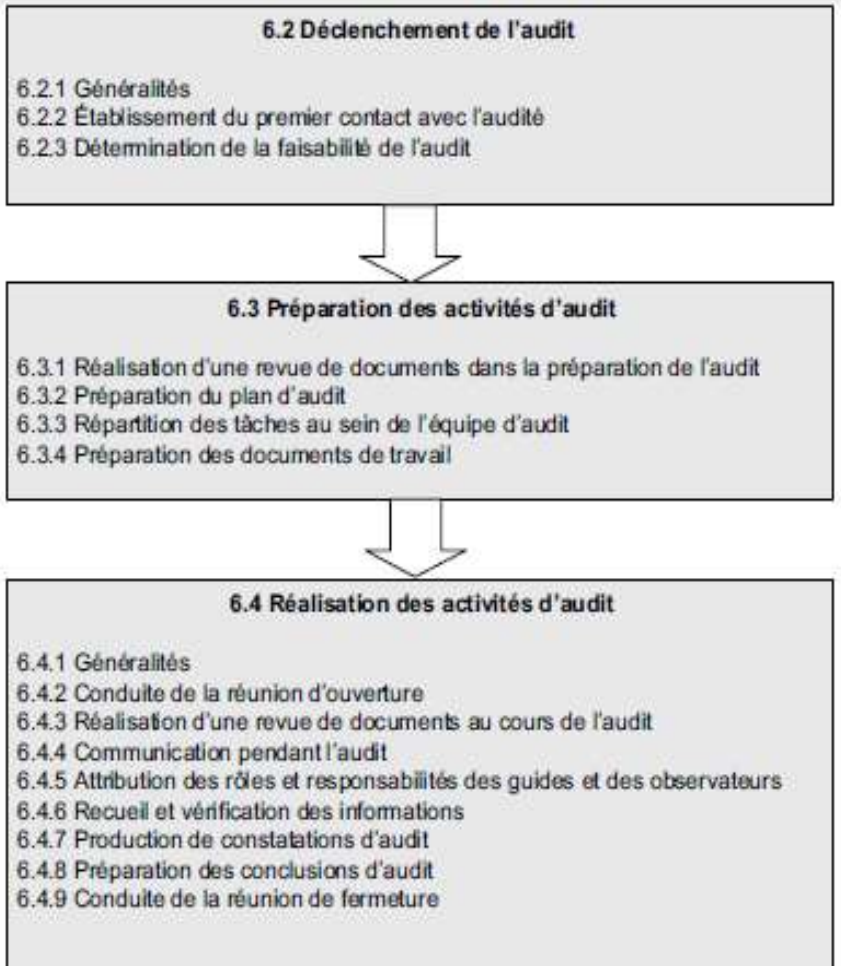
Après

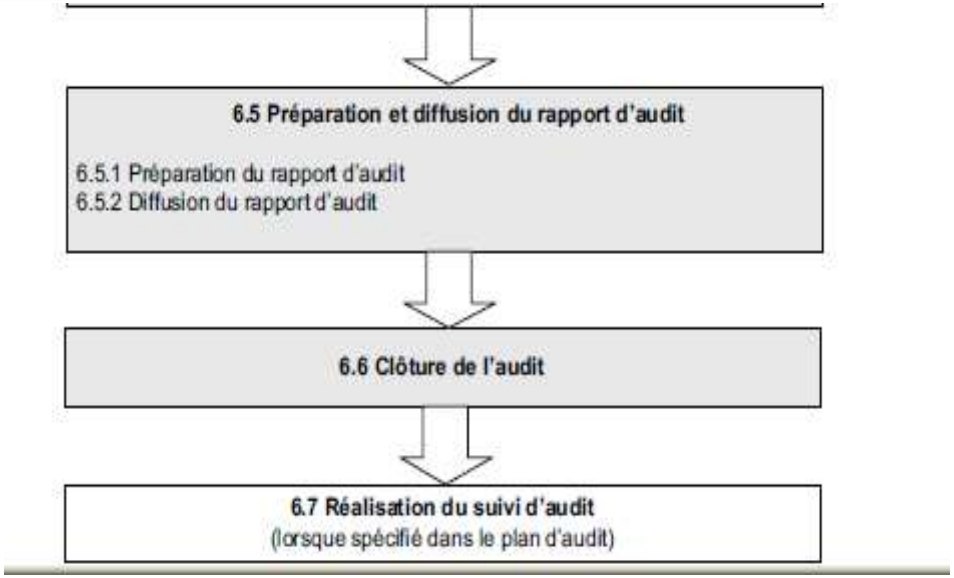
- Préparation, approbation et diffusion du rapport d'audit
- Clôture de l'audit
- Suivi d'audit

Le déroulement d'un contrôle



Le déroulement d'un contrôle





⇨ **Démarche ISO19011**

Audit & contrôle

Le déroulement d'un contrôle

⇨ **Démarche issue de l'ISO19011**

Le cadrage d'un contrôle

⇨**Lancement du contrôle**

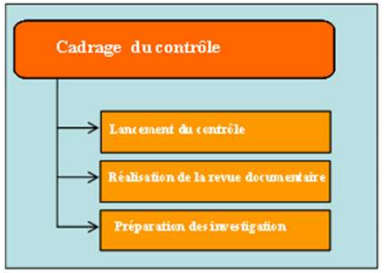
- ✓ Constitution de l'équipe
- ✓ Objectifs et périmètre,
- ✓ Référentiel et risques à évaluer
- ✓ Nature des investigations
- ✓ Organisation, contacts

⇨**Revue documentaire**

- ✓ Recueil et analyse des documents, procédures
- ✓ Recueil des précédents audits

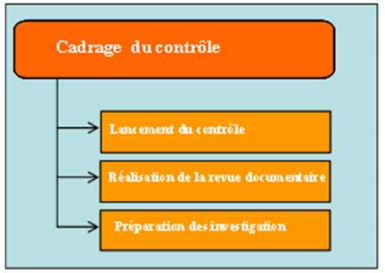
⇨**Préparation des investigations**

- ✓ Logistique,
- ✓ planning, …



Le cadrage d'un contrôle

Lancement d'un contrôle – Pt clefs

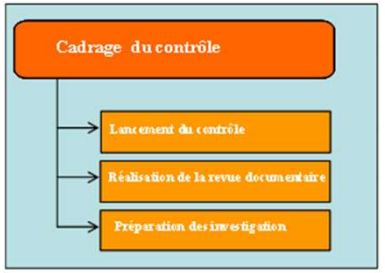


⇨ Constitution de l'équipe de contrôle
- ✓ Bien identifier les compétences nécessaires
- ✓ Langues, compréhension du contexte culturel
- ✓ Aptitude à communiquer
- ✓ Indépendant (absence de conflit d'intérêt par exemple)

⇨ Faisabilité
- ✓ Existante d'informations disponibles et suffisantes
- ✓ Bon niveau de coopération avec l'audité
- ✓ Disponibilité des ressources
- ✓ Planning

Le cadrage d'un contrôle

Lancement d'un contrôle– Pt clefs

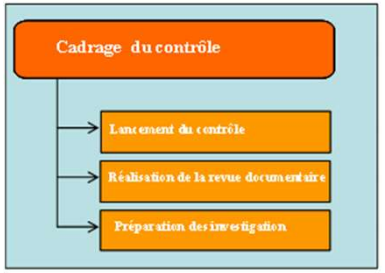


⇨ Premiers contacts

- ✓ Bien identifier les flux de communication
- ✓ Transparence sur les objectifs, l'équipe, le planning, …
- ✓ Demander l'accès aux documents
- ✓ Recueillir les contraintes logistiques
- ✓ Mettre en place un protocole de confidentialité si nécessaire

Le cadrage d'un contrôle

Revue documentaire – Pts clefs



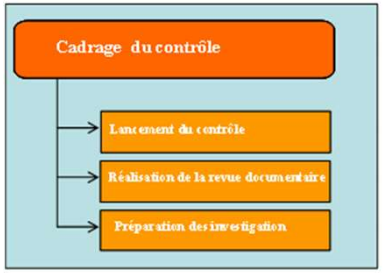
⇨ Vérifier la validité des documents :

- ✓ Approuvés,
- ✓ En vigueur
- ✓ …

⇨ Déterminer la conformité documentaire du système par rapport au référentiel de contrôle

Le cadrage d'un contrôle

Préparation des investigations sur site (ou plan d'audit) – Points clefs



⇨Logistique

⇨Planning détaillé

⇨Rôles des intervenants

⇨Contraintes (langues, logistique, …),

Le plan d'audit doit

- ✓ Clarifier au maximum le déroulement de l'audit
- ✓ Etre validé par les différentes parties
- ✓ Etre stable

Le cadrage d'un contrôle

Plan d'audit : Contenu minimal

⇨Rappel des objectifs, critères, champs

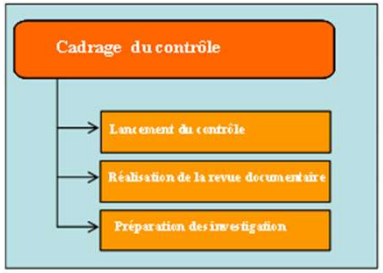
⇨Rôle de chaque auditeur/expert de l'équipe

⇨Répartition des tâches

⇨Dates et lieux des activités d'audits sur site

⇨Ressources allouées chez l'audité

⇨Logistique de l'audit sur site (accès, transport, …)



Rédacteur

⇨Réalisé par le responsable de l'équipe d'audit

⇨Approuvé par le client de l'audit

⇨Présenté et accepté par l'audité

Le cadrage d'un contrôle

Chaque auditeur doit

- ⇨ Connaître sa mission précise
  - ✓ Validé avec le responsable d'audit
- ⇨ Constituer et préparer :
  - ✓ Listes type et plan d'échantillonnage d'audit
  - ✓ Formulaires d'enregistrement des informations
  - ✓ Fiche d'écart, relevé de constatations
- ⇨ Conserver tous ses documents
  - ✓ Au moins jusqu'à la fin de l'audit
  - ✓ Sécuriser et maîtriser cette conservation

Cadrage d'un contrôle

Introduction

Périmètre et objectif

- Dispositifs concernés
- Objectifs à atteindre

Démarche appliquée

- Méthode et démarche générale
- Nature des contrôles
- Échelle d'évaluation

Méthode de travail

- Entretiens et investigations techniques
- Investigations documentaires
- Actions en cours

Conditions d'interventions

- Pilotage et intervenants
- Échanges entre les parties
- Planning

Cadrage d'un contrôle

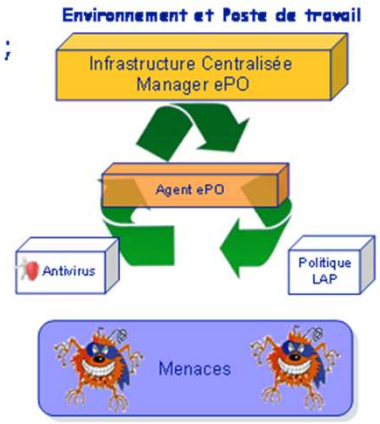
Dispositif concerné

L'infrastructure antivirale permet la mise en œuvre de la Politique Antivirale. Cette infrastructure propose les principales fonctions suivantes :

- La détection des infections virales ;
- Le routage des pollutions vers la surveillance centralisée ;
- La gestion du parc en terme de protection ;

mais également

- la diffusion et la mise à niveau des signatures ;
- l'établissement de statistiques et de tableaux de bord.



L'infrastructure s'appuie sur

- Une couche « centralisation » utilisant la solution ePO (Mc afee) ;
- Une couche « solution antivirale » :
  - une pour les environnements MS Windows (VirusScan);
  - une pour les environnements Linux (LiniuxShield).

Cadrage d'un contrôle

Périmètre et objectifs du contrôle

Périmètre :

Technique :

- Serveur BdD;
- Serveurs Managers (5 à 8 serveurs);
- Serveurs Référentiels distribués (90 serveurs);
- Firewall.

Organisationnel et procédural :

- Gestion d'habilitation;
- Administration fonctionnelle;
- Exploitation du logiciel et du socle;
- La gestion des mises à jour;
- Modes dégradés et continuité d'activité;
- Le processus de sauvegarde;
- Gestion des traces;
- Surveillance.

Objectifs :

- Contrôler le niveau de conformité de l'infrastructure et l'organisation associée par rapport au référentiel de sécurité;
- Evaluer l'adéquation du niveau de sécurité offert avec les besoins DICT définis;
- Identifier les principaux points FORTS et points FAIBLES;
- Proposer les ACTIONS d'amélioration à mettre en œuvre.

Contribuer à la démarche d'amélioration du niveau de sécurité de l'infrastructure anti-virale

Cadrage d'un contrôle

Démarche de contrôle de sécurité de la DSI

Lancement, cadrage

Objectifs, nature du contrôle, périmètre technique et fonctionnel, logistique, plan de contact, planification des investigations...

Contrôle de sécurité

CS1 Contrôler les Infrastructures	CS2 Contrôler les Applications	CS3 Contrôler les Process
→ **Analyse d'architecture** → **Contrôle de configuration** → Tests d'intrusion	→ Revue de code → **Tests des fonctions de sécurité** → Tests de vulnérabilités	→ Contrôle des environnements → **Contrôle des procédures** → Contrôle des ressources

Restitution et Suivi

Formalisation du rapport, Présentation des résultats: point forts, points d'amélioration, recommandations

Cadrage d'un contrôle

Nature des contrôles à réaliser

Appréciation des processus de sécurité, notamment (non exhaustif)

- Gestion d'habilitation;
- Administration fonctionnelle;
- Exploitation du logiciel;
- La gestion des mises à jour;
- Les modes dégradés et la continuité d'activité;
- Le processus de sauvegarde;
- Gestion des traces;
- Supervision.

à travers des entretiens de 1h à 2h auprès des interlocuteurs suivants

- L'exploitation fonctionnelle ;
- L'exploitation technique d'ePO : Serveurs, firewall,… ;
- …

Appréciations techniques à travers

- Revue d'architecture;
- Les tests des principales fonctions de sécurité de la solution (plate-forme spécifique hors production);
- Le contrôle de configuration des éléments précités, notamment sur la base des éléments fournis par le contrôle opérationnel en place sur cette activité;

Investigations documentaires

Apprécier le niveau de sécurité en termes techniques et procéduraux

Recueillir les éléments nécessaires aux réponses attendues par l'IG

1

Cadrage d'un contrôle

Entretiens et investigations techniques

Etape 1 : Réunion de présentation architecture : Alain et Martine 03/05 à 15h
Etape 2 : Entretiens et Investigation :

Rôle	Nom	Date	Lieu	Entretien	Relevé technique	Durée
Responsable de service	DPI/SPS/SES Alain	9-10/05	Nancy	Ok	S.O.	1h
Exploitation fct : ePO et LAP	DPI/SPS/SES Martine	9-10/05	Nancy	Ok	S.O.	2h
Config et paramétrage ePO	DPI/SPS/SES	9-10/05	Nancy	S.O.	Tests fonctionnels	1 j
Exploitation fct : Projet et processus	DPI/SPS/SES Eric	9-10/05	Nancy	Ok	S.O.	2h
Exploitation technique : socle	DPI/MTD/EMD Stephane	9-10/05	Nancy	Ok	DPI/SPS/AMT JM	2h
Exploitation technique : Sonde de détection	DPI/SPS/SES Philippe	9-10/05	Nancy	Ok	DPI/SPS/AMT	1h
Exploitation technique : BdD	DPI/MTD/MCO Sergiy		Ivry	Ok	DPI/SPS/AMT	1h
Exploitation technique : Firewall	DPI/MTD/CRC Marie-Laure		Toulouse	Ok (visio)	DPI/SPS/AMT	1h
Administration Locale	DET/GCA/AMT / Nadjim		Ivry	Ok	S.O.	1h

Rem : les relevés de configuration pourront être réalisés majoritairement à partir de Nancy

Cadrage d'un contrôle

Analyse documentaire

Documents en attente

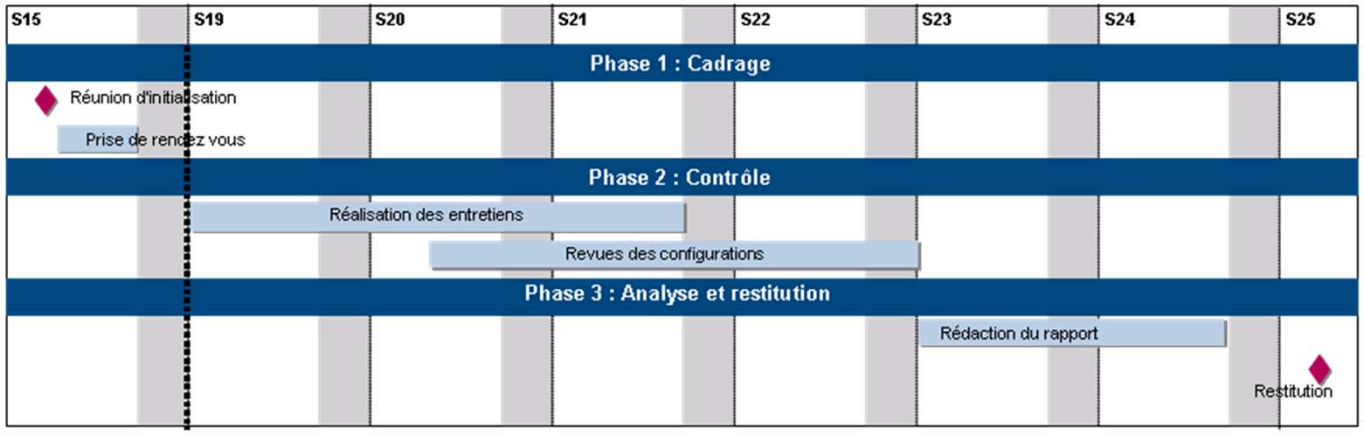
- Organigramme du projet
- Analyse de risques du projet / Qualification des besoins / Exigences de sécurité
- Gestion des tiers (ex : maintenance, intervention, ...)
- Description technique de la solution (DAT, schéma de flux)
- Liste des échanges/flux avec les applications
- Procédure d'habilitation des administrateurs / exploitants
- Procédures d'exploitation (sauvegarde, mise à jour, incident, aliénation)
- PRI / PCA et comptes-rendus des éventuels tests réalisés

Cadrage d'un contrôle

Conditions d'intervention

Planning cible :

Lancement : 06 Avril
Réunion de présentation architecture :
Investigations Nancy : 9 et 10 Mai
Investigation Ivry et TLS : courant Mai
Restitution Fin Juin



Cadrage d'un contrôle

Conditions d'intervention

Actions en cours

- Accréditation + badge auditeurs : date limite 06/02
- Réservation salle de réunion période d'audit
- ...

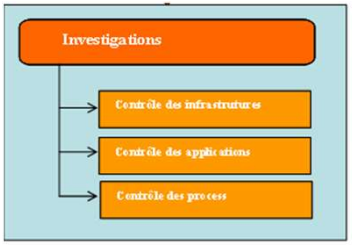
Pilotage et intervenants

- Pilote du contrôle:
  - Christophe X
- Intervenants en charge du contrôle:
  - Auditeurs fonctionnel : Mr Durant
  - Auditeurs technique : Mr Dupont

Échanges entre les parties

- Comptes rendus des entretiens : soumis à validation sous 8j
- Rapport final : transmis protégé par zip + mot de passe
- Contacts privilégiés :
  - Christophe X
  - Patrick D

Les investigations



⇨**Réunion d'ouverture (sur site)**

- ✓ Rappel des objectifs et du périmètre
- ✓ Présentation de la manière dont les activités seront menées
- ✓ Réponse aux questions des intervenants concernés
- ✓ Confirmation du planning

⇨**Investigations (tout ou partie)**

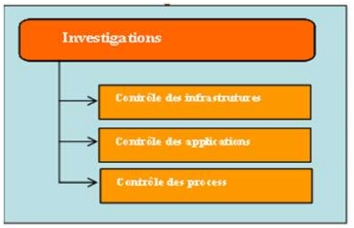
- ✓ Contrôle des infrastructures
- ✓ Contrôle des applicatifs
- ✓ Contrôle des processus

⇨**Réunion de clôture : restitution à chaud**

- ✓ Mise en évidence des premiers constats du contrôle

Les investigations

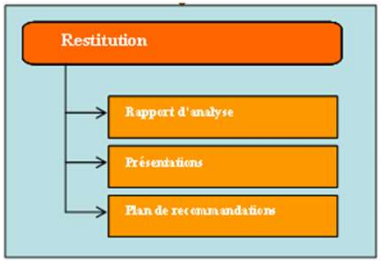
Réunion d'ouverture – Pts clés



⇨**Réunion d'ouverture (sur site)**

- ✓ Tour de table, présentation de l'équipe, identification des personnes
- ✓ Confirmation de l'objectif, rappel de la démarche
- ✓ Confirmation des circuits de communication
- ✓ Besoin de guides
  - logistique,
  - organisation RdV,
  - accompagnement, …
- ✓ Confirmation du planning (dates et horaires)
- ✓ Communication en cours de contrôle
  - pt à la fin de la journée ou pt à chaque fin de semaine,
  - alerte en cas de constat grave,
  - traitement des difficultés, …

La restitution



- **Élaboration d'un rapport de contrôle détaillé constituant le résultat analytique**
  - ✓ Conformité / Non conformité
  - ✓ Points forts / points faibles
- **Présentation des principales preuves**
- **Restitution détaillée au cours d'une présentation basée sur le rapport de contrôle**
- **Plan de recommandations structuré**
  - ✓ Rapport cout-contrainte / efficacité

La restitution : constats

Les non-conformités sont notifiées :

- en écart majeur s'il s'agit d'un non-respect d'au moins une exigence certifiée et qui fait courir un risque direct et significatif sur le système,

- en écart mineur s'il s'agit d'un non-respect, à un moment donné, d'une exigence certifiée, et qui fait courir un risque limité sur le système,

- en remarque s'il s'agit :

- d'un dysfonctionnement potentiel non décelé dans l'analyse des risques ou

- qui ne fait pas l'objet d'une exigence dans le(s) texte(s) de référence, et qui fait courir un risque limité sur le système,

- d'une inadéquation entre la situation constatée et les exigences de certification qui n'affecte pas directement le système,

- d'un fonctionnement qui permet seulement d'atteindre partiellement les objectifs et qui nécessite une amélioration du système.

La restitution : constats

LSTI

Fiche d'écart n

Remarque	✓	Non-conformité mineure		Non-conformité majeure	

Constat/Ecart

Conséquences et risques induits :

Références documentaires :

Date	Nom & prénom de l'auditeur/du Responsable d'audit	Signature

Commentaire de l'audité

Actions correctives et/ou préventives

Délai de mise en œuvre :

Date	Nom & prénom du responsable de la mise en œuvre des actions	Signature

Efficacité des actions correctives et/ou préventives planifiées

Date	Nom & prénom de l'auditeur/du Responsable d'audit	Signature

Vérification : documentaire		visite sur site		Fiche d'écart : soldée		non soldée		partiellement soldée	

Evaluation de la mise en oeuvre des actions correctives et/ou préventives

Date	Nom & prénom de l'auditeur/du Responsable d'audit	Signature

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

Points clés

- Le plan de contrôle organise et planifie les activités de contrôle à court et moyen termes en fonction des risques.
- Un contrôle se déroule selon une démarche normalisée.
- La qualité de la phase de cadrage conditionne la réussite du contrôle.
- Les constats doivent être appréciés en fonction du risque