Ecole de Management Strasbourg

UNIVERSITÉ DE STRASBOURG

www.em-strasbourg.eu

Module 2: Gestion de la sécurité du S.I.

Octobre 2019

Sommaire

I) Introduction

II) La gestion des risques informatiques

- l'analyse des risques liés au S.I.

III) Mesures organisationnelles

- politique de sécurité et procédures
- fonction RSSI
- classification de l'information
- gestion des risques liés à la sous-traitance

IV) Organisation de la sécurité par processus

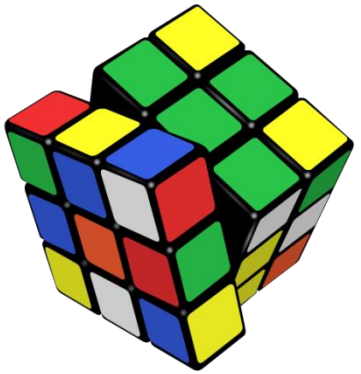
- Processus de gestion des incidents
- Processus de gestion des changements
- Processus de gestion des accès

IV) Cadres de référence: modèle et standards

- CobiT
- ISO/IEC 27001:2005 et 27002:2005
- Modèles de maturité

V) Exemple: modèle type pour la mise en place d'une stratégie de sécurité

I) INTRODUCTION



Quels sont les principaux types d'incidents de sécurité?

- **Quelques statistiques (2018):** (entreprises de plus de 100 salariés)

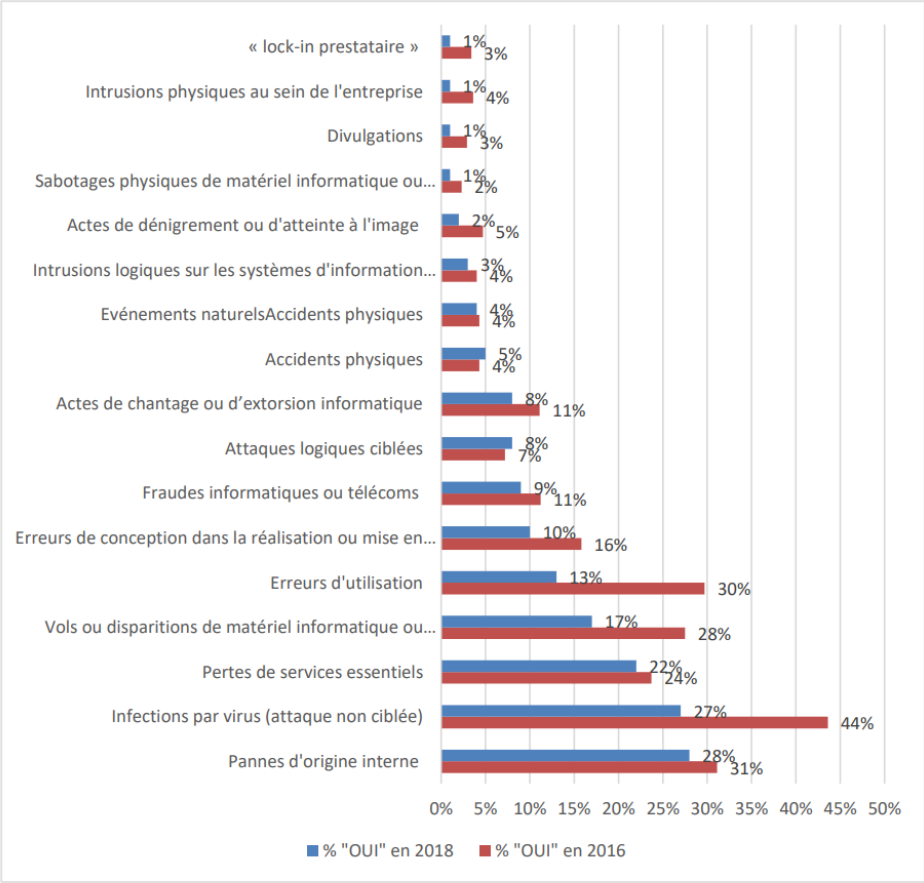


Figure 40 - Comparaison des fréquences d'incidents entre 2016 et 2018 (périmètre 2016)

A retenir:

- Des incidents de diverse nature
- Qui évoluent dans le temps
- Ciblés et non-ciblés
- Qui peuvent être accidentels ou intentionnels (p. ex. malveillance, vol)
- Causés par des facteurs internes ou externes
- Ayant des causes organisationnelles; techniques (p. ex. pannes, disfonctionnements) ou liées au facteur humain (p. ex. erreur de saisie, erreur non-intentionnelle).

Une variété qui impose de connaître les principaux risques pour établir une stratégie de traitement des risques.

Au cours de l'année 2017, votre entreprise a-t-elle subi des incidents de sécurité de l'information consécutifs à...

Source: CLUSIF – Rapport 2018

Approche

- **Sécuriser les informations – pas seulement une démarche technique:**
  - Optimiser l'utilisation des ressources pour réduire les risques.

  - Nécessité d'une approche globale:
    - Eléments techniques
    - Eléments organisationnels
    - Eléments humains

⇨ Les mesures de sécurité à mettre en place dépendent de l'activité de l'organisation, de la réglementation et des contraintes de son écosystème.

⇨ Afin d'évaluer le niveau de sécurité attendue, les questions suivantes peuvent être posées :

- Qu'est ce que je veux protéger ?
- De quoi je veux me protéger ?
- A quel type de risques mon organisation est-elle exposée ?
- Qu'est ce que je redoute ?
- Quelles sont les normes qui s'appliquent à mon organisation ?

Approche

- **Eléments clés pour gérer la sécurité du S.I.** (« security framework »)
  - Connaître les risques

    Analyse des risques:
    - menaces, vulnérabilités, probabilité de survenance, conséquences possibles

  - Etablir un plan de réduction des risques

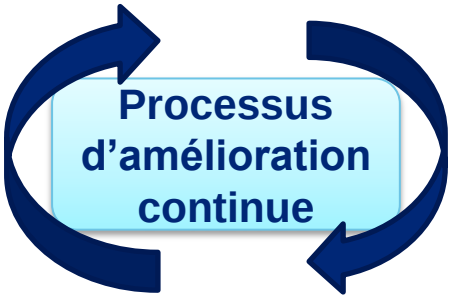
    Plan de réduction des risques: intégrer les éléments techniques, organisationnels, (politiques, procédures, processus…), et humains (formation, sensibilisation)

  - Mettre en place des contrôles alignés sur les risques

    Mise en œuvre d'un environnement de contrôle

  - S'assurer de l'efficacité des contrôles

    Monitoring: s'assurer que les contrôles atteignent les objectifs fixés et sont appliqués.

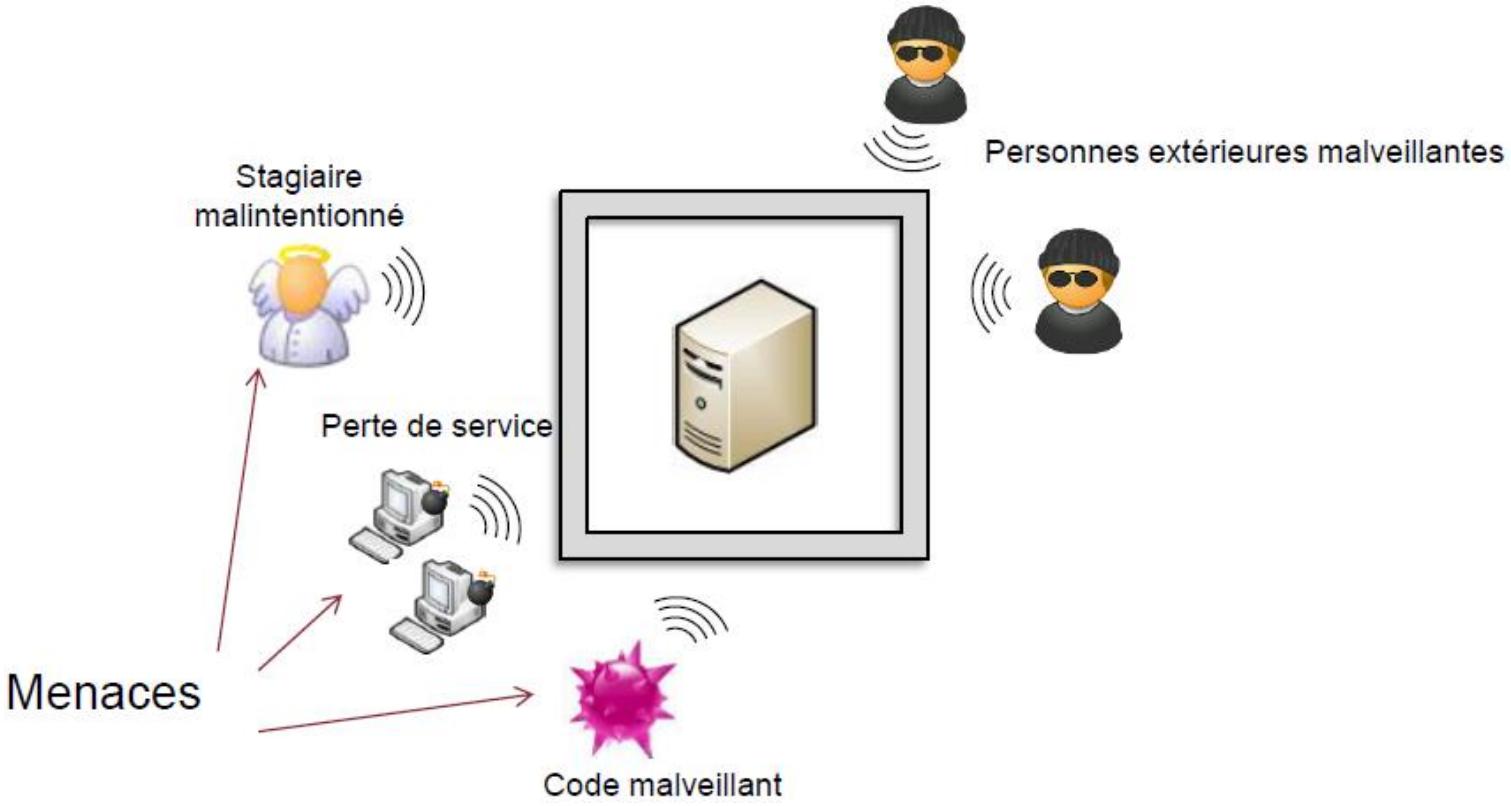


II) La gestion des risques informatiques

- l'analyse des risques liés au S.I.

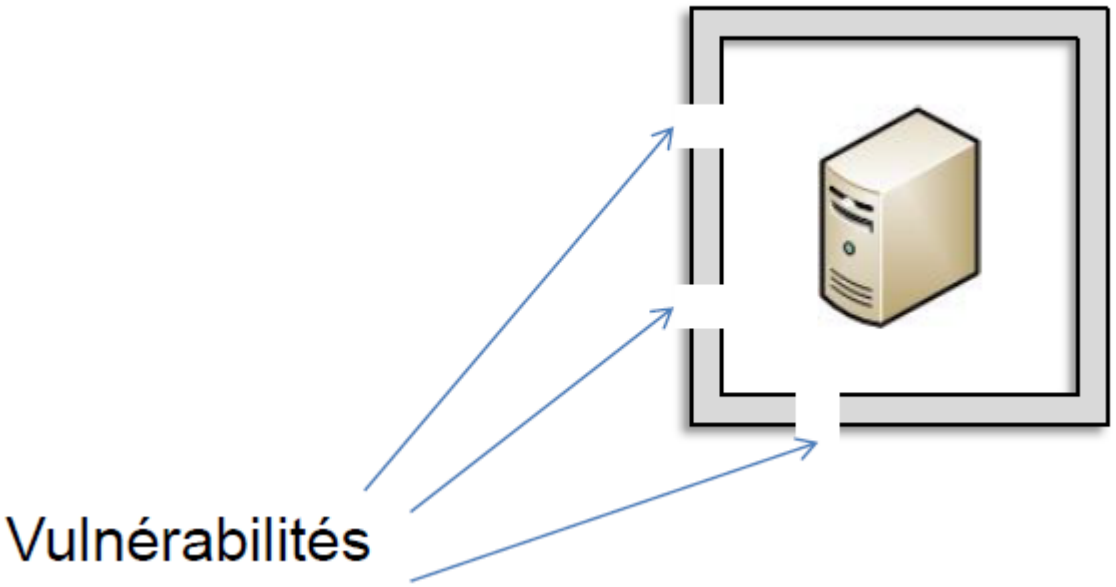
Notion de « Menace »

- **Cause potentielle d'un incident**, qui pourrait entrainer des dommages sur un bien si cette menace se concrétisait.



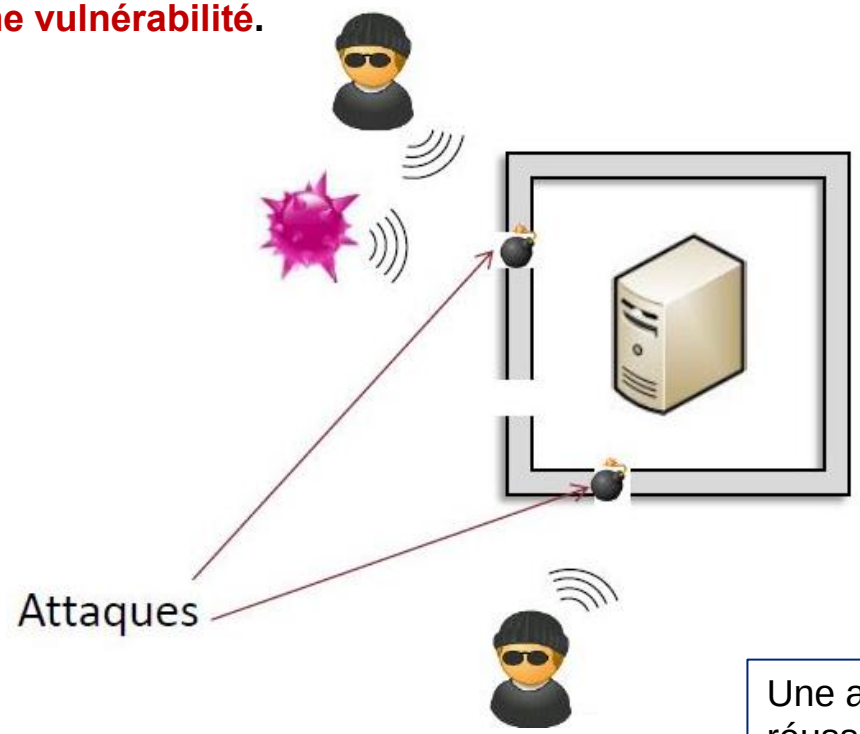
Notion de « Vulnérabilité »

- **Faiblesse au niveau d'un bien** (au niveau de la conception, de la réalisation, de l'installation, de la configuration ou de l'utilisation du bien).



Notion d'« Attaque »

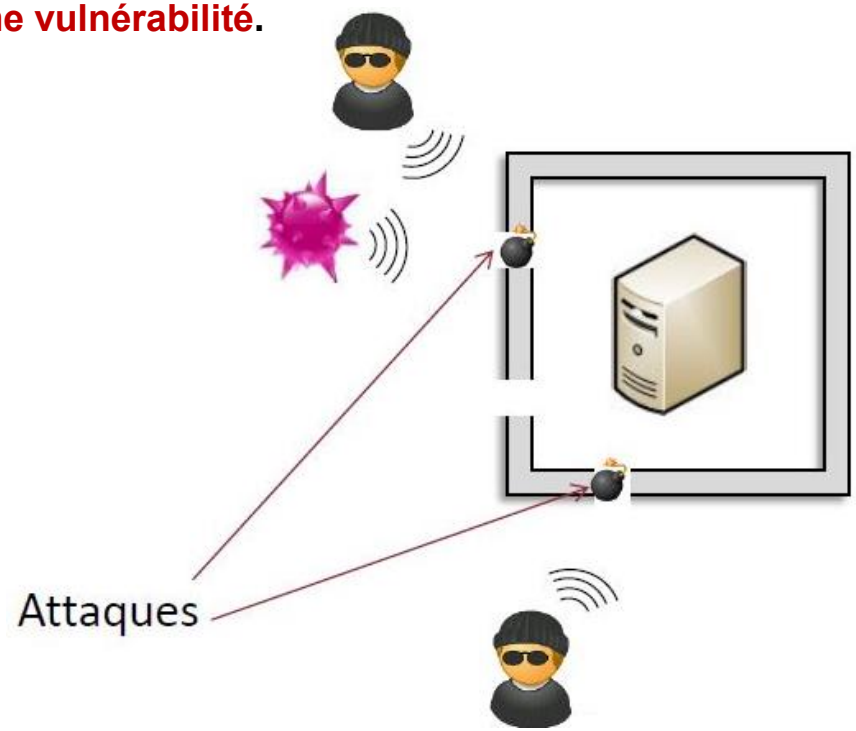
- **Action malveillante destinée à porter atteinte à la sécurité d'un bien. Une attaque représente la concrétisation d'une menace, et nécessite l'exploitation d'une vulnérabilité.**



Une attaque ne peut donc avoir lieu (et réussir) que si le bien est affecté par une vulnérabilité.

Notion d'« Attaque »

- **Action malveillante destinée à porter atteinte à la sécurité d'un bien. Une attaque représente la concrétisation d'une menace, et nécessite l'exploitation d'une vulnérabilité.**



Une attaque ne peut donc avoir lieu (et réussir) que si le bien est affecté par une vulnérabilité.

Ainsi, tout le travail des experts sécurité consiste à s'assurer que le S.I. ne possède aucune vulnérabilité.
Dans la réalité, l'objectif est en fait d'être en mesure de maitriser ces vulnérabilités plutôt que de viser un objectif 0 inatteignable.

La gestion des risques informatiques
L'analyse des risques liés au S.I.

Exemples de menaces:

- Accès au réseau par des personnes non-autorisées.
- Non-conformité avec la réglementation.
- Perte de confidentialité de mots de passe.
- Incendie.
- Erreur de maintenance.
- Changements non-autorisés
- Fraude
- Vol d'information
- Ingénierie Sociale
- Installation de logiciels non-autorisés
- Utilisation non-autorisée de logiciels
- Accès physiques non-autorisés
- Interruption de processus Métier

Etc.

Exemples de vulnérabilités:

- Mots de passe par défaut non-changés
- Gestion des mots de passe non-appropriée
- Formation insuffisante des utilisateurs.
- Ségrégation des tâches insuffisante.
- Tests de validation logicielle insuffisants.
- Bâtiments exposés aux incendies.
- Droits d'accès non-revus.
- Employés non-motivés.
- Redondance insuffisante des S.I.
- Sauvegardes logicielles irrégulières ou non-testées.
- Téléchargements depuis l'Internet non contrôlés.
- Absence de politique de gestion des accès.
- Absence de séparation entre environnements de Test et de Production

Etc.

La gestion des risques informatiques
L'analyse des risques liés au S.I.

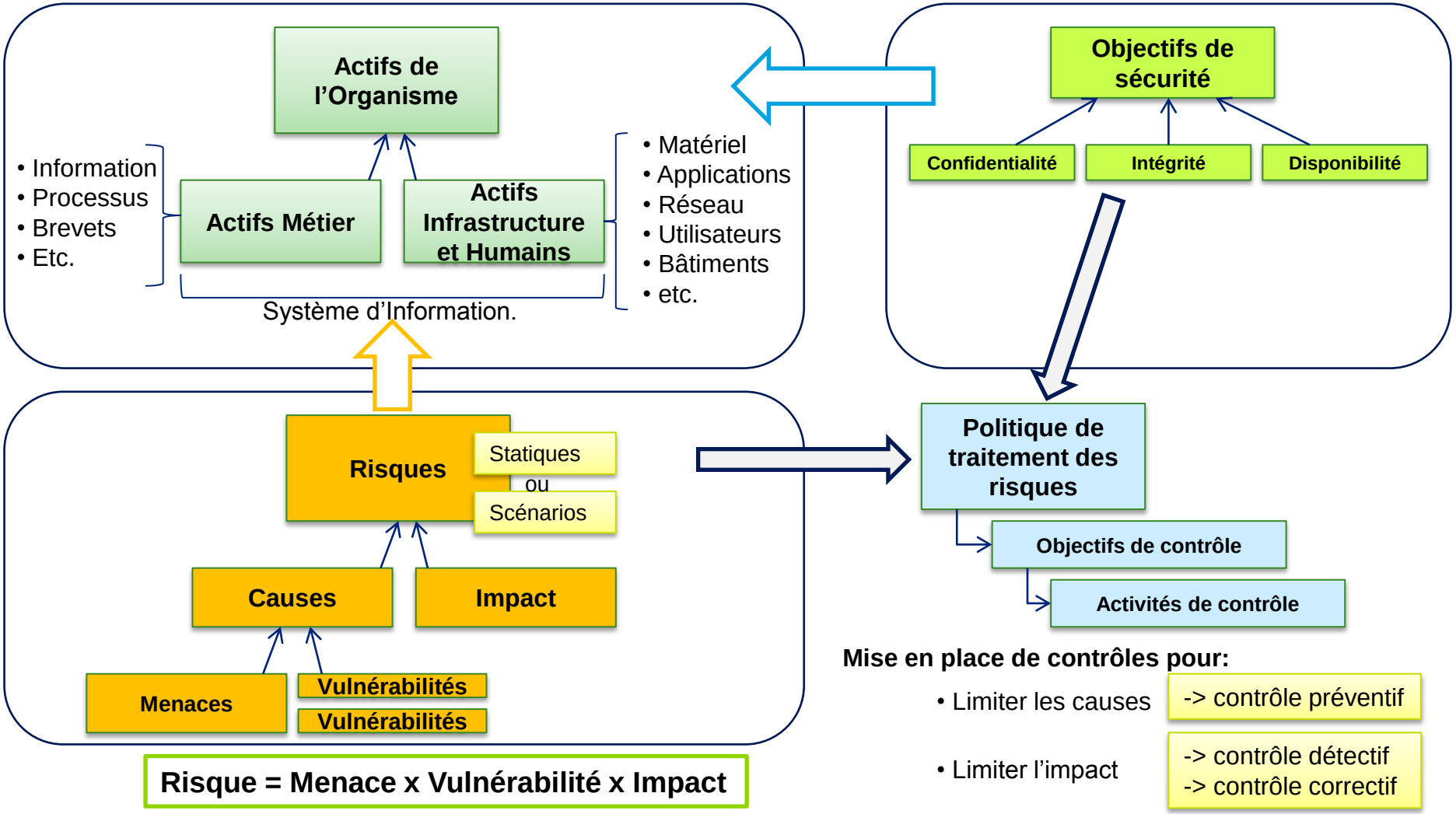
- **Contexte de l'analyse des risques informatiques:**
  - **Un Organisme dispose d'Actifs (ressources) ayant une valeur et nécessaires pour atteindre des objectifs Métier.**
    - Exemples d'Actifs « tangibles « et « intangibles »: Informations (sur différents supports), méthodes, processus, personnel, systèmes d'information (matériel, applications, réseau, bases de données), bâtiments, etc.
  - **Les Actifs sont soumis à des Menaces affectant la *Confidentialité*, l'*Intégrité* et la *Disponibilité* des Actifs:**
    - Accidents, Erreurs humaines, malveillance, etc.
  - **Les Actifs présentent des Vulnérabilités spécifiques face aux menaces (vulnérabilité = faille pouvant être exploitée par une Menace)**
    - Ex: Menace = incendie, Vulnérabilité = Bâtiments exposés aux incendies.
  - **Les vulnérabilités peuvent entrainer des incidents (non-intentionnels) ou des attaques (internes ou externes), plus ou moins fréquents, ce qui provoque des dysfonctionnements, plus ou moins importants.**

CLUSIF: « Le risque est la conjonction d'un actif, d'une menace susceptible de faire subir un dommage à cet actif et de vulnérabilités exploitées par la menace pour faire subir à l'actif ce dommage. »

  - **L'analyse de risques a pour but d'évaluer la probabilité d'occurrence d'une attaque et l'impact du dysfonctionnement, afin de permettre de choisir et justifier les mesures de sécurité adaptées:**
    - Techniques
    - Organisationnelles
    - Juridiques

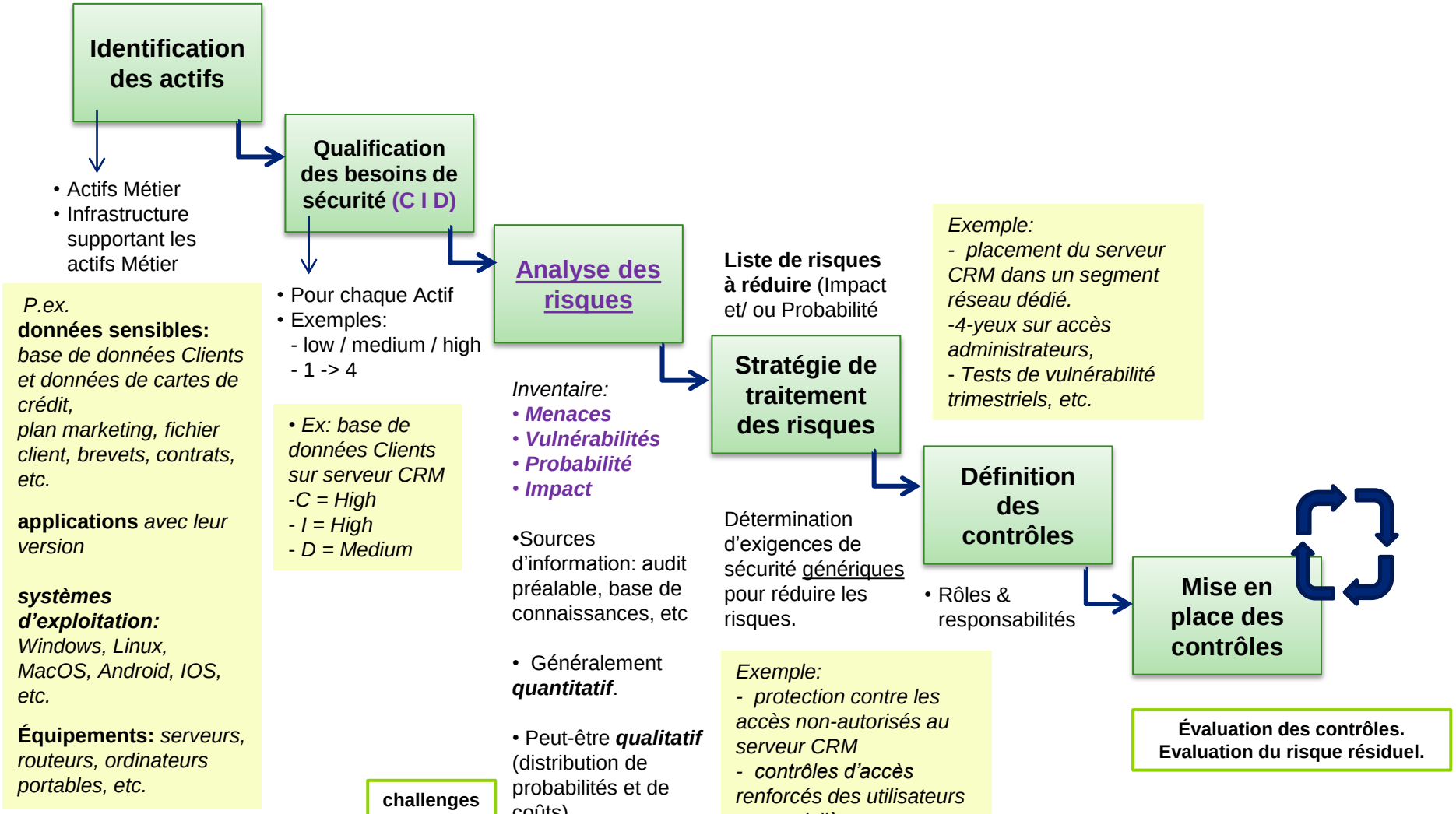
La gestion des risques informatiques
L'analyse des risques liés au S.I.

- **Concepts de la gestion des risques informatiques**



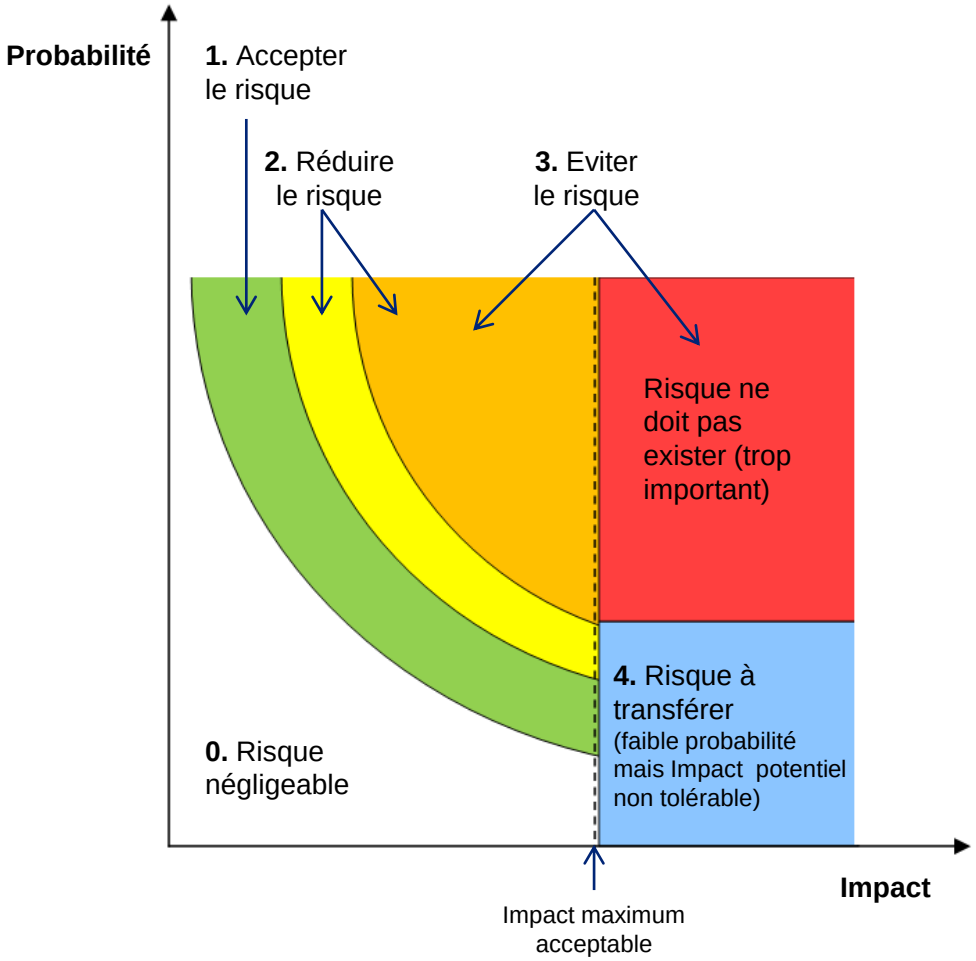
La gestion des risques informatiques
L'analyse des risques liés au S.I.

- **Processus (générique) de gestion des risques**



La gestion des risques informatiques
L'analyse des risques liés au S.I.

- **Les stratégies de traitement des risques:**



Pour chaque risque identifié lors de l'analyse:

Option 1. Accepter le risque:
- Analyse coût / bénéfices (ex: si coût supérieur aux pertes potentielles).
- Acceptation doit être basée sur une analyse formelle.

Option 2. Réduire le risque
- Réduire l'Impact et/ ou la Probabilité à un niveau « acceptable ».
- Ex: contrôles renforcés, amélioration des processus Métier, limites, alertes, sous-traitance à un spécialiste, etc.

Option 3. Eviter / refuser le risque
- Ex: risque réglementaire ou financier trop important, ressources ou infrastructures insuffisantes pour gérer le risque, etc.
- Effet de bord: perte d'opportunités.

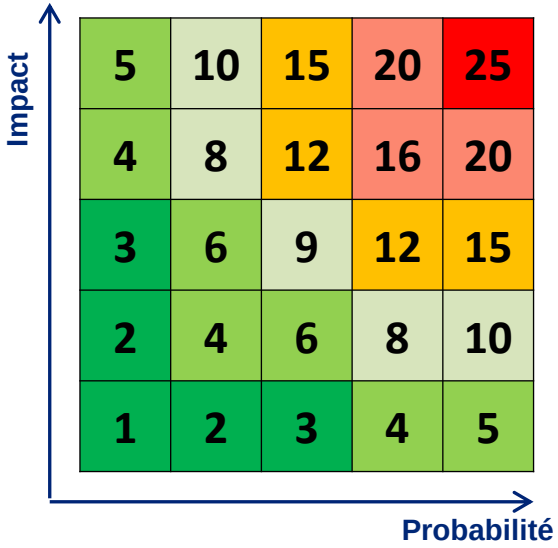
Option 4. Transférer le risque:
- Impact important mais probabilité faible *(ex: incendie)*
- Transfert par sous-traitance & assurances

- **Exemples de matrices d'évaluation des risques**

1. Exemple de matrice Impact x Probabilité

Impact (estimé)	**Elevé**	Moyen	Elevé	Elevé
	Moyen	Faible	Moyen	Elevé
	Faible	Faible	Faible	Moyen
		Faible	**Moyen**	**Elevée**
		Probabilité (estimée)		

2. Exemple de grille 5x5 de détermination du risque



16 - 25	Non-autorisé
12 - 15	Haute-priorité, à traiter absolument
8 - 10	A revoir au moment opportun
1 - 6	Risque acceptable

La gestion des risques informatiques
L’analyse des risques liés au S.I.

- **Exemple - formalisation de l’analyse des risques:**

Sécurité logique - Introduction

• Liens et références

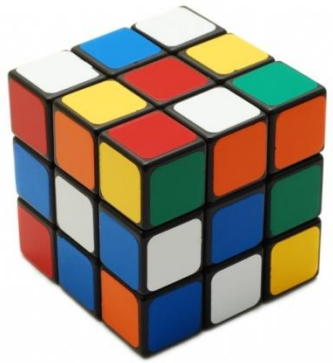
L’analyse des risques liés au S.I.

- **CLUSIF: La gestion des risques – Concepts et méthodes**
  https://clusif.fr/publications/gestion-des-risques-concepts-et-methodes/

- **Nicolas Mayer: La gestion des risques pour les systèmes d’information**
  (présentation des méthodes EBIOS, MEHARI, OCTAVE)
  http://www.nmayer.eu/publis/NMA-JPH_MISC24.pdf

III) Mesures organisationnelles

- politique de sécurité et procédures
- fonction RSSI
- classification de l'information
- gestion des risques liés à la sous-traitance
- audits de sécurité



La politique de sécurité

Mesures organisationnelles
La politique de sécurité du système d'information (PSSI)

Avant de mettre en place des procédures ou des mesures techniques visant à augmenter la sécurité d'un organisme, il importe de procéder à une analyse des risques et de rédiger une **politique de sécurité**. La politique de sécurité sert à formaliser et à coordonner toutes les démarches organisationnelles et techniques de sécurité de l'organisme.

- **Eléments clés de la PSSI:**
  - Document établissant la démarche de sécurisation du S.I.
    - Doit être précédée d'une **analyse des risques** (même sommaire).
    - Permet de définir les **actifs** informatiques (processus, informations, applications, etc.) ayant une valeur pour l'entreprise et à quelles **vulnérabilités** (exploitées par des menaces) ils sont exposés.
    - Permet de mettre en évidence des **objectifs** de sécurité et les **mesures** comportementales, organisationnelles et techniques attendues.
    - Permet de **sensibiliser** tous les utilisateurs aux exigences de sécurité de l'Organisme.
  - Pas de solution « clé en main »: choisir une approche pragmatique, adaptée à la taille et à la **criticité** des actifs (ex: pour une PME, la PSSI sera un document court et concis, centré sur un objectif d'amélioration continue).
    - S'inspirer des bonnes pratiques (ex: **ISO/IEC 27001** et **ISO/IEC 27002**) et les adapter.

- **Procédures et bonnes pratiques:**
  - Eléments critiques pour définir le cadre de gestion de la sécurité de l'information
  - Définissent les **rôles, responsabilités, objectifs et processus** au sein de l'Organisation
  - Doivent être régulièrement **revues, MAJ et diffusées** (sensibilisation des employés concernés)

Mesures organisationnelles

La politique de sécurité du système d'information (PSSI) - Exemples

- **Exemple de politique de sécurité:**
  https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/infSecPol.pdf (document public)

- **Exemples de procédures informatiques:**
  https://info.lse.ac.uk/staff/services/Policies-and-procedures (documents publics)

- **Liens et références:**

  ANSSI - **guides et recommandations de l'ANSSI**
  http://www.ssi.gouv.fr/administration/bonnes-pratiques/

  exemples:
  - Sécuriser un site web,
  - Sécuriser les accès wi-fi,
  - Définition d'une politique de pare-feu,
  - Sécuriser son ordiphone,
  - Comprendre et anticiper les attaques DDOS, etc.

  CASES (Luxembourg)

  - **L'approche RSSI – présentation détaillée de ce que doit contenir une politique de sécurité**
    https://www.cases.lu/knowhow/CISOApproach_fr.html

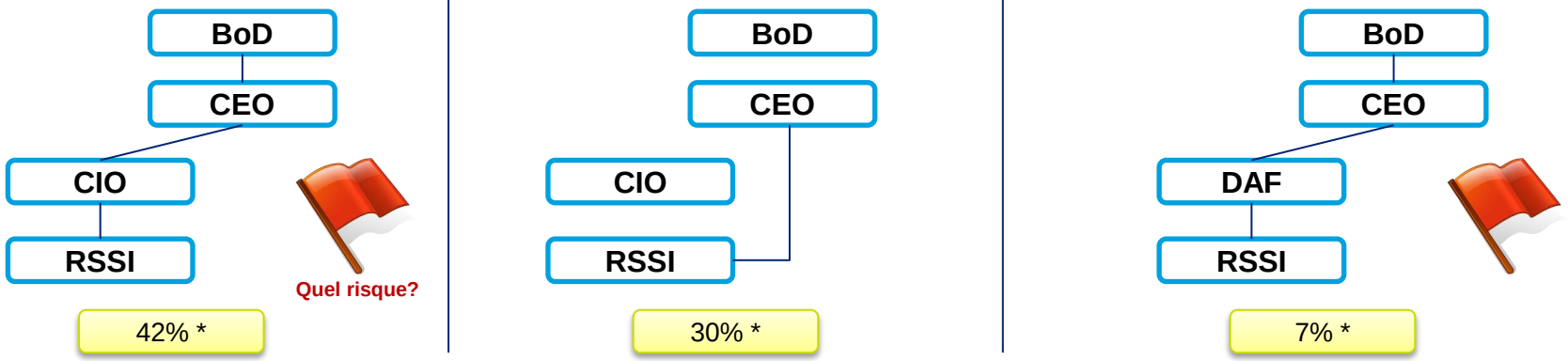
La fonction RSSI

Mesures organisationnelles

Le RSSI (Responsable de la Sécurité des SI) (a.k.a. CISO, ex. « Security Officer »)

- Présent dans 67% des entreprises*
- Rôle conceptuel et (fréquemment) opérationnel:
  - Responsable du maintien de la sécurité de l'information au cours de son cycle de vie.
  - Protection des données sensibles (ex: données personnelles)
  - Suivi de la conformité des S.I. avec les exigences réglementaires (ex: PCI DSS)
  - Veille technologique / suivi des nouvelles menaces (cyber-sécurité)
  - Rôle de validation dans la gestion des accès (ex: profils avec privilèges, recertification des utilisateurs, etc.)
  - Sensibilisation des utilisateurs aux problématiques de sécurité (« first line of defence »)
  - Intervient dans la gestion des projets (définition / validation des aspects sécurité)
  - Intervient dans la gestion de la continuité (plan de secours, plan de continuité), fréquemment comme coordinateur.

- Positionnement du RSSI:



- Fonction qui évolue vers le rôle de « Risk Manager ».

*Source: CLUSIF 2016

Mesures organisationnelles
Le RSSI (Responsable de la Sécurité des SI)

- **Quelques statistiques (2018):**
  (entreprises de plus de 100 salariés)

Identification et de l'attribution de la fonction RSSI:

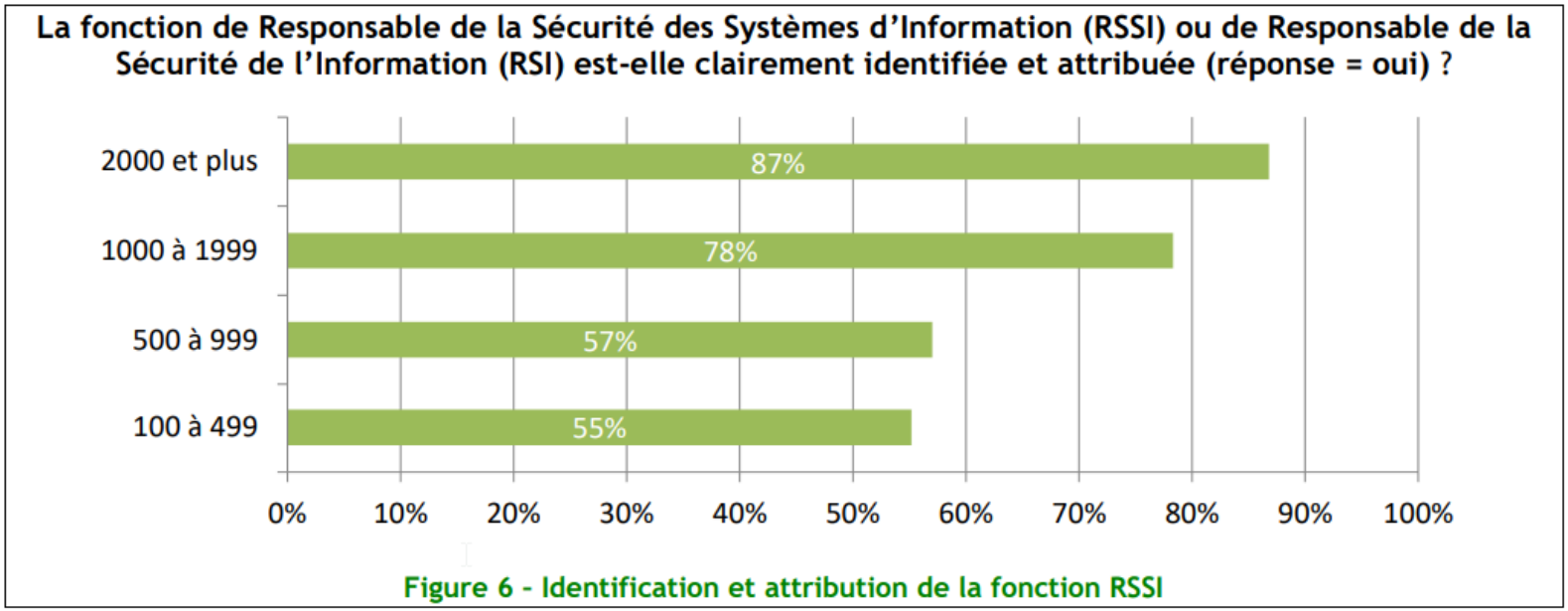


Figure 6 - Identification et attribution de la fonction RSSI

Source: CLUSIF – Rapport 2018

Mesures organisationnelles
Le RSSI (Responsable de la Sécurité des SI)

- **Quelques statistiques (2018):**
  (entreprises de plus de 100 salariés)

Effectif total de l'équipe sécurité permanente au sein de l'entreprise:

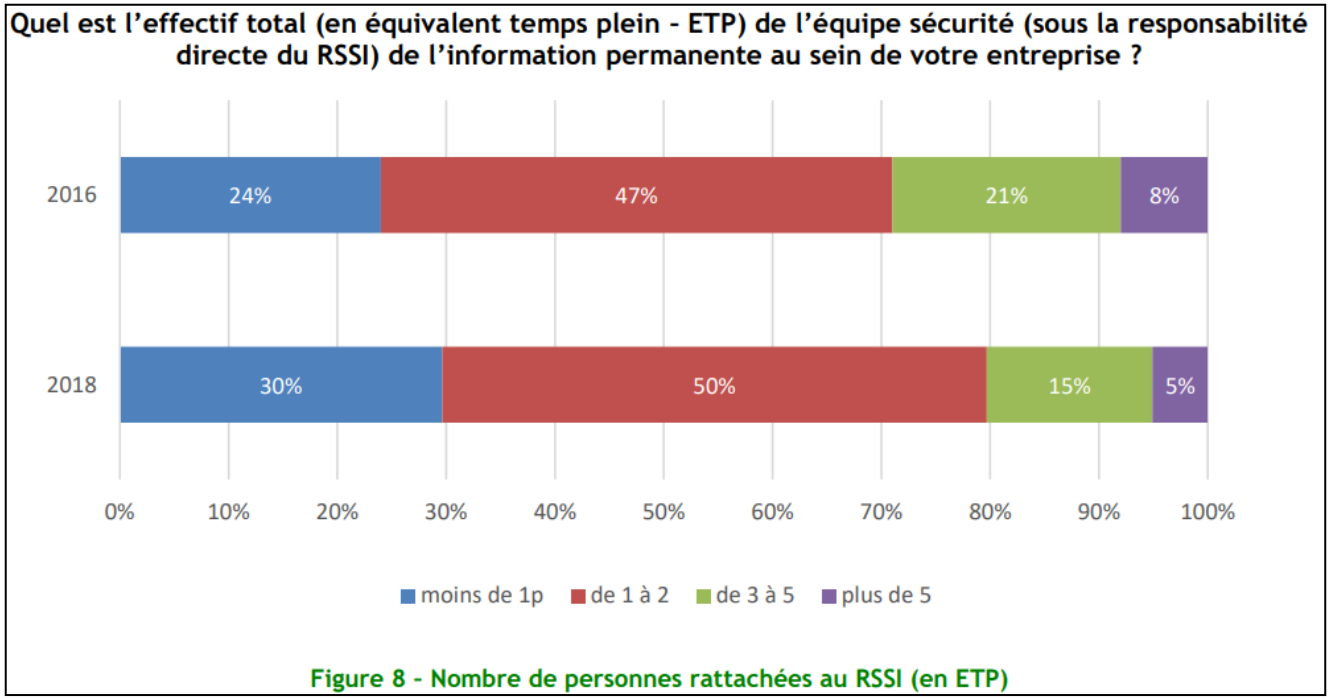


Figure 8 - Nombre de personnes rattachées au RSSI (en ETP)

« Quand la fonction de RSSI n'est pas attribuée, elle est en très grande majorité (les 2/3) assurée par le Directeur des Systèmes d'information ou le Responsable informatique. »

Source: CLUSIF – Rapport 2018

Mesures organisationnelles
Le RSSI (Responsable de la Sécurité des SI) (suite)

- **Quelques statistiques (2018):**
  (entreprises de plus de 200 salariés)

Quel est le rattachement hiérarchique du RSSI au sein de votre entreprise ?

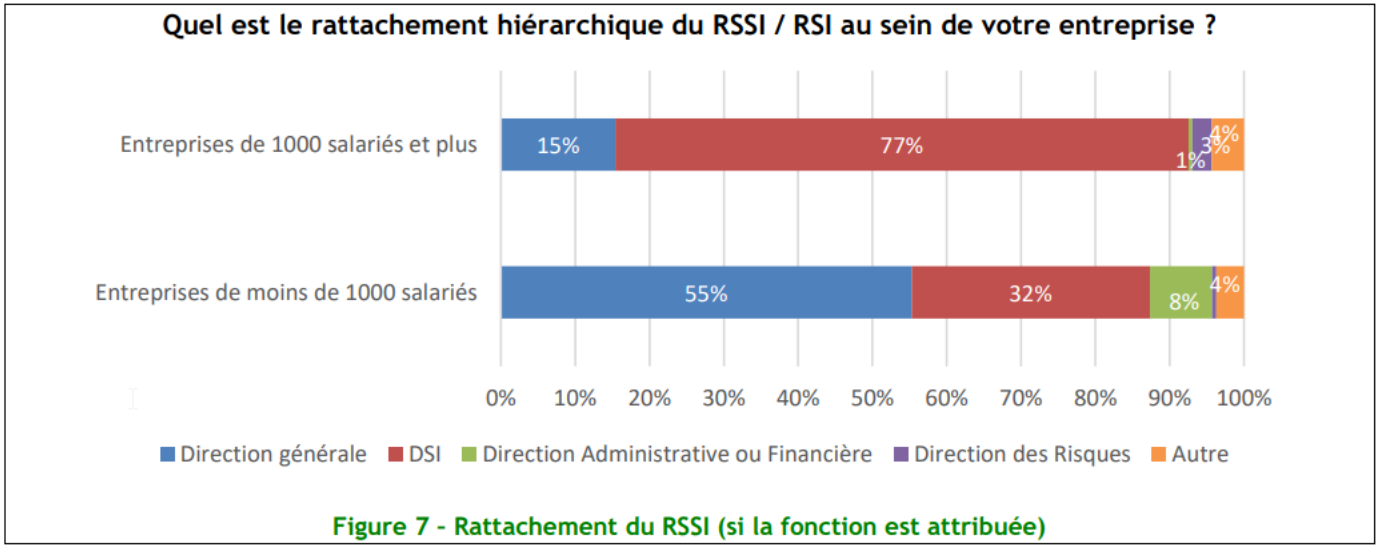


Figure 7 - Rattachement du RSSI (si la fonction est attribuée)

« Le RSSI, quand la fonction est attribuée, est rattaché majoritairement soit à la Direction Générale soit à la DSI, avec une répartition différente selon la taille de l'entreprise»

Temps consacré aux différents aspects de la fonction par le RSSI

Le temps consacré aux différents aspects de sa fonction, par le RSSI ressort ainsi :

Aspects fonctionnels (Politique, analyse de risques, etc.)	25%
Aspects techniques (architecture de sécurité, suivi de projets, etc.)	30%
Aspects opérationnels (gestion des droits, administration, etc.)	25%
Aspects juridiques (charte utilisateurs, recherche de preuve, etc.)	09%
Aspects de communication (sensibilisation, etc.)	11%

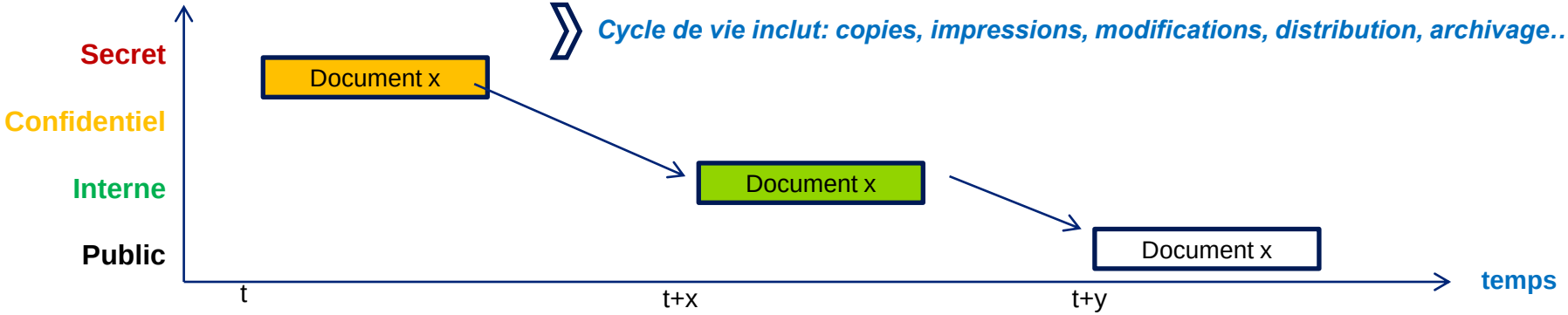
Source: CLUSIF – Rapport 2018

Classification de l'information

Mesures organisationnelles
Classification de l'information

« On ne protège bien que ce que l'on connaît bien »

- **Contexte:**
  - L'information constitue un actif majeur pour toute Organisation.
  - L'information connait divers niveaux de sensibilité, qui évoluent au cours de son cycle de vie.



⇒Une démarche structurée de gestion de l'information est de plus en plus attendue par les régulateurs (directement ou indirectement). Ex: Autorité fédérale de surveillance des marchés financiers (FINMA) en Suisse.

- **Objectif:**
  - Protéger l'information contre un emploi inapproprié et susceptible nuire à l'entreprise.
  - Assurer un niveau de sécurité homogène et cohérent:
    - En fonction de la sensibilité de l'information.
    - Tout au long de son cycle de vie
  - Agir en tant que contrôle préventif visant principalement à limiter les erreurs humaines.

Une bonne compréhension de la classification et une adhésion des utilisateurs est fondamentale (rôle du RSSI).

Mesures organisationnelles
Classification de l'information

- Acteurs de la classification:
  1. **Propriétaire** des données: garant de la classification des informations.
  2. **Dépositaire:** responsable du respect des principes de classification.
  3. **Utilisateur:** manipulation de l'information en accord avec les principes de classification.

- En pratique: chaque propriétaire doit valider des **catégories** d'information, auxquelles sont associées des **règles comportementales** en fonction du niveau de classification.

- Exemple de classification (basée sur la Confidentialité) - *simplifiée*

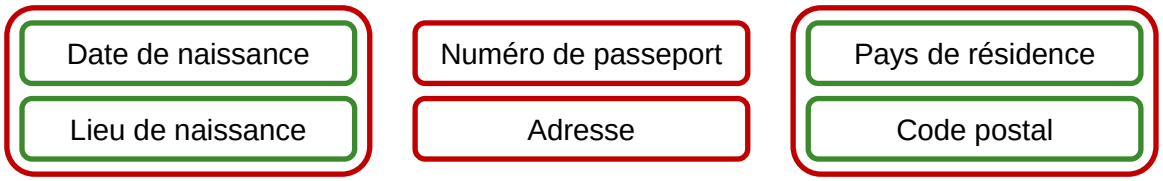
Classe (confidentialité)	**Définition et description**	Exemples de règles comportementales
Secret	Informations secrètes à caractère hautement confidentiel (ou pouvant influencer le marché). Ex: projet stratégique, résultats financiers avant publication, etc.)	Conservation sous forme chiffrée. Accès nominatif uniquement. Pas d'échange par e-mail.
Confidentiel	Informations dont la divulgation peut avoir des conséquences graves (ex: amendes / procès). Accès restreint à des personnes ayant un motif valide.	Accès restreint (« need to know ») à certains groupes d'utilisateurs. Echange par e-mail obligatoirement chiffré.
Interne	Documents internes à l'organisation ou liés à un projet.	Pas de communication hors de l'Organisation ou des membres du projet (sauf accord explicite).
Public	Informations facilement accessibles en dehors de l'Organisation (ex: article de presse, site web, etc.)	Accès et distribution sans restriction. Respect des règles de copyright.

Exemple

Mesures organisationnelles
Classification de l'information

- Eléments à prendre en compte dans la classification:
  1. L'**agrégation** de données peut influencer la classification de l'information (exemple: données client protégées par le secret bancaire suisse*)

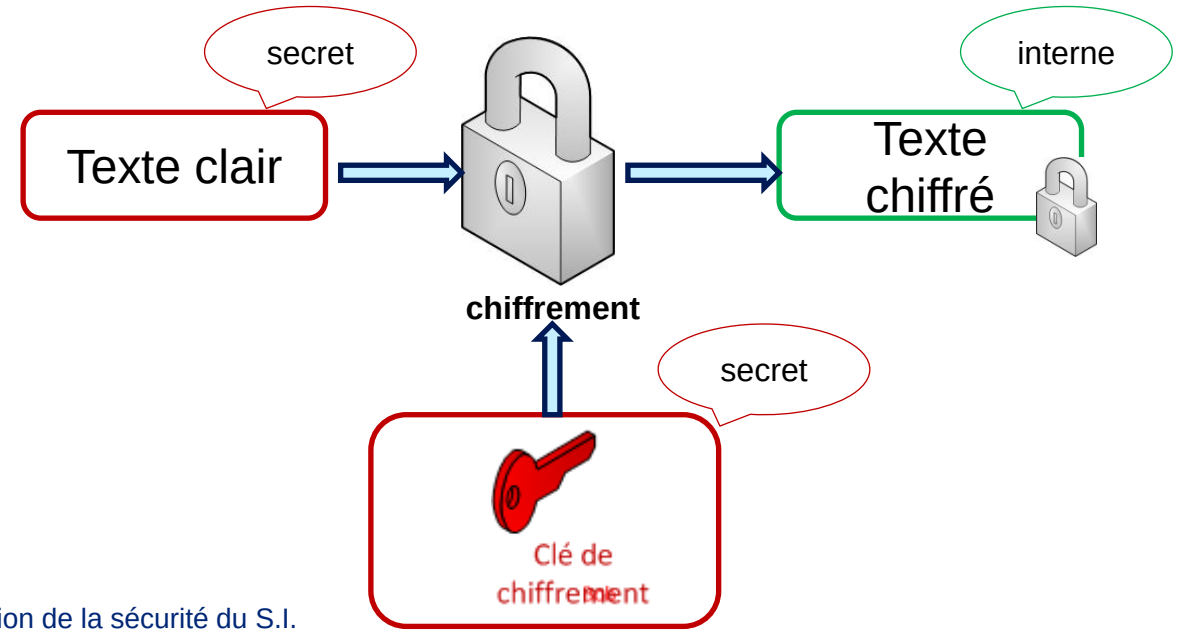
Référence: Publication FINMA (Mars 2013) distingue 3 types de données:
•« direct CID »
• « indirect CID » *(document number)*
• « potentially indirect CID ».



Donnée non confidentielle

Donnée confidentielle (seule ou agrégée)

  2. Le **chiffrement** des données influence la classification:



Gestion des risques & sous-traitance

Mesures organisationnelles

Gestion des risques liés à la sous-traitance

- **Contexte et objectifs de la sous-traitance informatique**
  - Spécialisation des Organisations sur leur cœur de Métier (généralement non-IT).
  - Réduction / Maîtrise des coûts via la sous-traitance (à nuancer).
  - Transfert du risque sur un tiers par l'externalisation (à nuancer).

- Types de sous-traitance:
  - Auprès d'un tiers spécialisé.
  - Intra-groupe.
  - En cascade.

  } (potentiellement à l'étranger)

  - Cas particulier du travail intérimaire.

QUIZZ Risques et challenges liés à la sous-traitance:

1. Risques opérationnels lié aux processus sous-traités

2. Risques liés à la **continuité** des activités sous-traitées

3. Non-conformité réglementaire / Contractuelle

4. Perte de **confidentialité** /

Exemples de risques associés:

Dépendance excessive envers le sous-traitant (« vendor lock-in »)

Sous-traitance en cascade non-maîtrisée et perte de contrôle

Hébergement de données sensibles à l'étranger

Contrôle interne du sous-traitant pas en ligne avec les exigences de l'Organisme

Plan de continuité du sous-traitant pas en ligne avec celui de l'Organisme

Hébergement de données sensibles à l'étranger

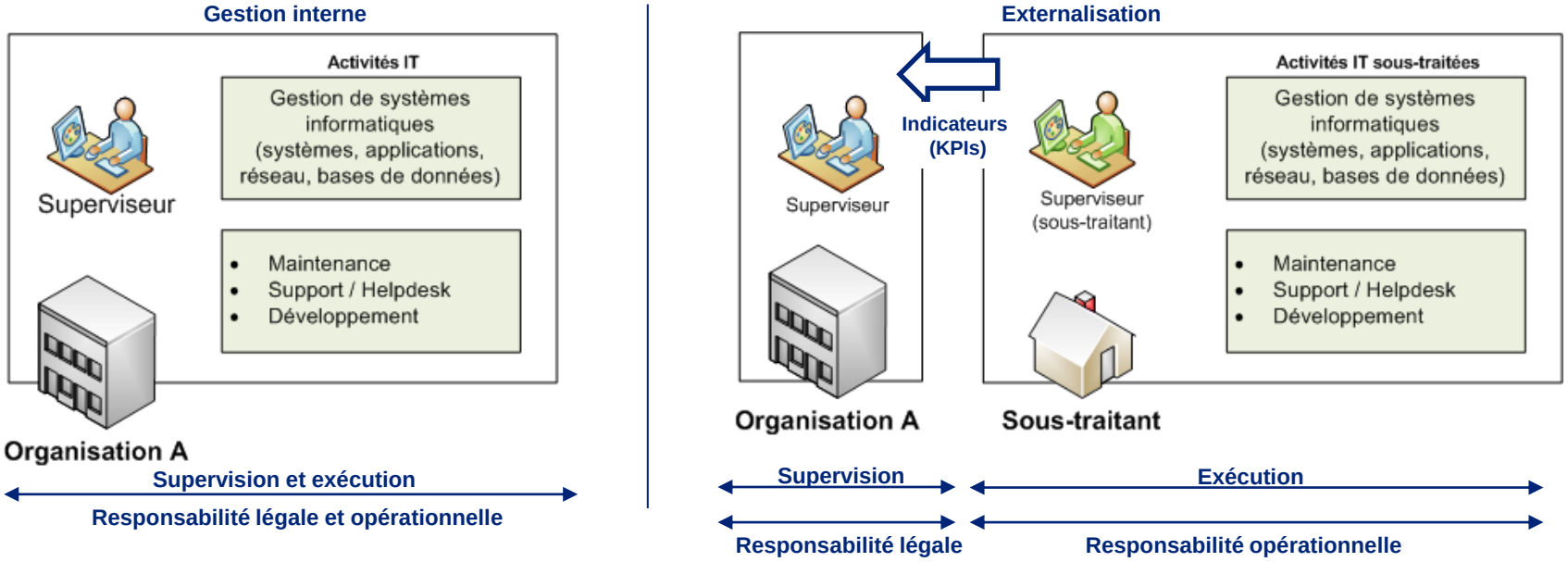
Accès non-autorisés par le personnel du sous-traitant

Etc…

Mesures organisationnelles

Gestion des risques liés à la sous-traitance

- **Exemple de sous-traitance informatique**



Outils de suivi de la sous-traitance:

- Maintien d'une structure interne de gestion de la sous-traitance (au minimum 1 personne + délégué).
- **Indicateurs** périodiques (KPIs) préparés par le sous-traitant.
  - > rapport mensuel sur les niveaux de services
  - > rapport quotidien sur les incidents
- **Inspections** périodiques du sous-traitant par le délégataire.
- **Audit du sous-traitant** par le délégataire ou par un tiers mandaté par le délégataire.
- **Audit interne du sous-traitant**.
- **Rapports d'Assurance** produits par le sous-traitant (ex: ISAE 3402) à destination de ses clients.

Mesures organisationnelles
Gestion des risques liés à la sous-traitance

- **Bonnes pratiques pour la gestion de la sous-traitance informatique**

Pré-requis (préalable à la sous-traitance)

1. Politique de sous-traitance documentée et validée par le CA, définissant les conditions auxquelles certaines activités peuvent être sous-traitées (pré-requis).
2. Analyse des risques du projet de sous-traitance (financiers, opérationnels, légaux, de réputation).

Exigences type

3. Contrat de sous-traitance définissant clairement les rôles et responsabilités de chaque partie.
   - sous-traitance doit être révocable et transférable.
   - maintien du contrôle interne du délégataire (« droit d'audit »).
   - droit de sous-traitance « en cascade ».
   - exigences de continuité et niveaux de service.

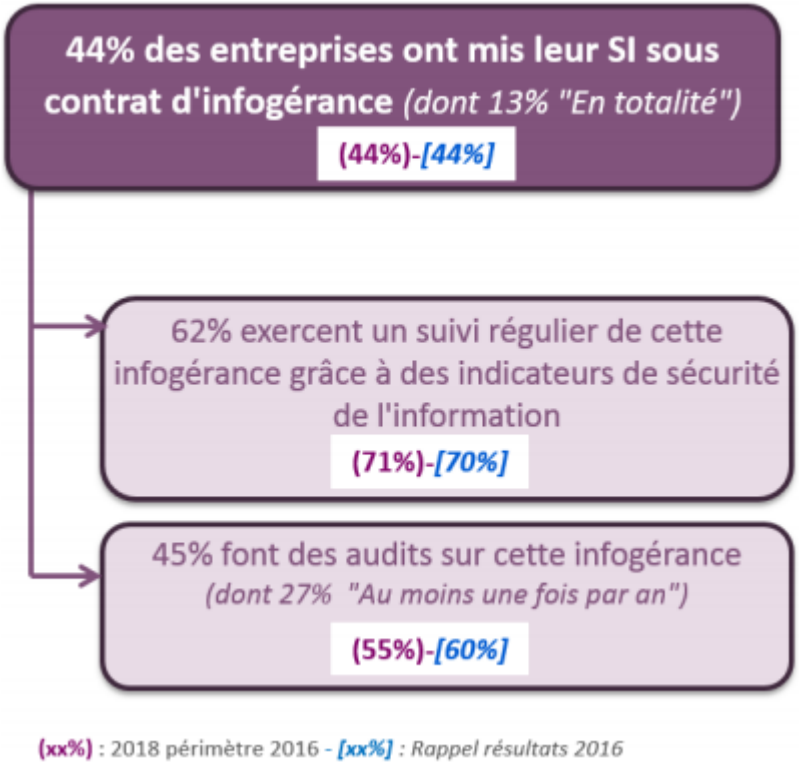
4. Prise en compte des aspects légaux (ex: protection de la vie privée).

5. Alignement du plan de continuité (prise en compte des risques liés à la sous-traitance, ex: rupture des lignes de communication avec le sous-traitant, dysfonctionnement prolongé au niveau du sous-traitant, etc.).

Mesures organisationnelles
Gestion des risques liés à la sous-traitance

- **Quelques statistiques (2018):**
  (entreprises de plus de 100 salariés)

Avez-vous placé tout ou partie de votre système d'information sous contrat d'infogérance ?



Part des SI sous contrat d'infogérance

44% des entreprises ont recours à l'infogérance.

On note même 13% d'entreprises qui ont une infogérance totale de leur SI.

Source:
CLUSIF – Rapport 2018

Mesures organisationnelles
Gestion des risques liés à la sous-traitance

- **Un outil de suivi de la sous-traitance : les Rapports d'Assurance (ex: SOC1, ISAE 3402, SOC2, SOC3)**

1. Norme internationale de référence pour évaluer les services de Tiers. Permet aux entreprises de s'assurer de la fiabilité des services fournis par des Tiers.
   - Pour une société prestataire de services: évite de multiplier les audits individuels de la part d'entreprises Clientes. Donne une bonne image en certifiant la qualité du contrôle interne.
   - Pour une société ayant recours à un/des prestataire(s): donne une assurance normalisée sur la qualité des contrôles internes mis en place par le(s) prestataires. Atteste de la mise en place de contrôle pertinents.

2. Rapports de contrôle des prestataires de services (rapports SOC)
   - l'auditeur indépendant exprime une opinion sur:
     – la description des contrôles par le prestataire ,
     – sur **la conception** *('design')* des contrôles pour atteindre certains objectifs de contrôle,
     – et sur **l'efficacité** du contrôle interne pour garantir avec une assurance raisonnable que les objectifs de contrôle ont été atteints sur une période donnée.

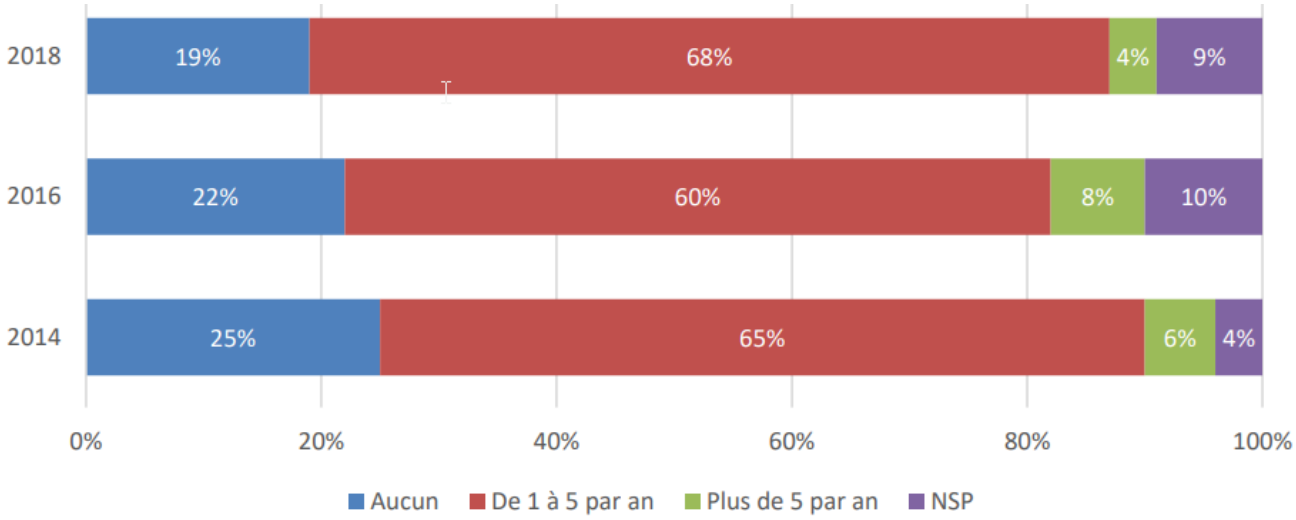
Exemple de rapport (SOC3 pour Amazon Web Services – 2018: https://d0.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf)

Les audits

Mesures organisationnelles
Les audits de sécurité

- **Quelques statistiques (2018):** (entreprises de plus de 100 salariés)

Combien d'audits ou de contrôles de sécurité du SI sont-ils menés en moyenne au sein de votre entreprise sur une période de 2 ans?



Source: CLUSIF – Rapport 2018

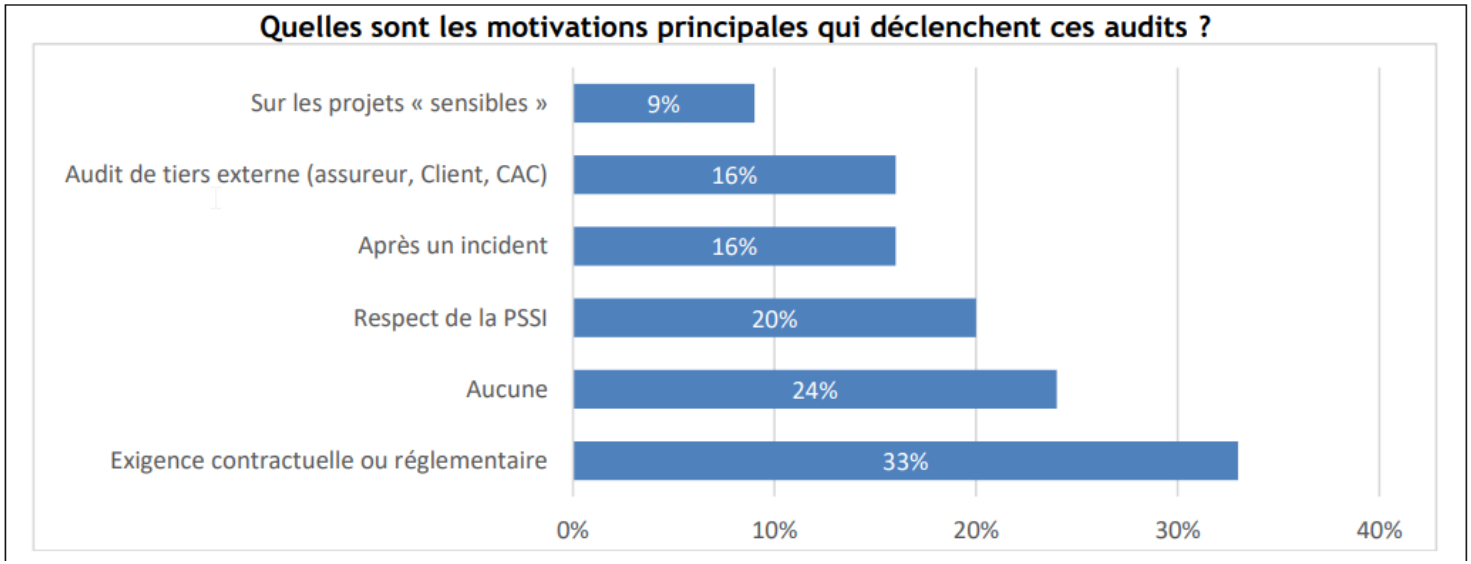
Nombre d'audits de sécurité du SI réalisés en moyenne par an

« Plus de deux tiers des entreprises interrogées ont réalisé au moins un audit de sécurité au cours des deux dernières années. Ces chiffres sont relativement stables depuis 2010 »

Les audits de sécurité

Source: CLUSIF – Rapport 2018

- **Quelques statistiques (2018):** (entreprises de plus de 100 salariés)



Motivations déclenchant des audits de sécurité

«Les grandes entreprises pratiquent les audits de façon quasi systématique (91% contre 68% en moyenne). Le secteur Banques-Assurances est également le plus consommateur de ce type de prestation (76%) contre seulement 55% dans le secteur Transports-Télécom.

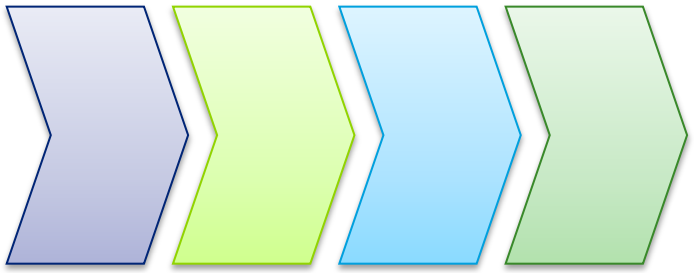
Les audits réalisés portent essentiellement sur les tests d'architecture (58%) et les tests d'intrusion (47%). Viennent ensuite les audits de configuration (45%), les audits organisationnels (39%) et les revues de droits d'accès logiques (34%), puis les audits de continuité d'activité (32%) et les audits physiques (30%).

En ce qui concerne les motivations de ces audits, l'existence d'une exigence contractuelle ou règlementaire est la première citée (33%). Viennent ensuite le respect de la PSSI (20%) puis à égalité l'audit de tiers externe et les suites d'un incident (16%).

Toutefois, 24% des répondant indiquent que les audits sont réalisés sans motivation particulière.»

IV) Organisation de la sécurité par processus

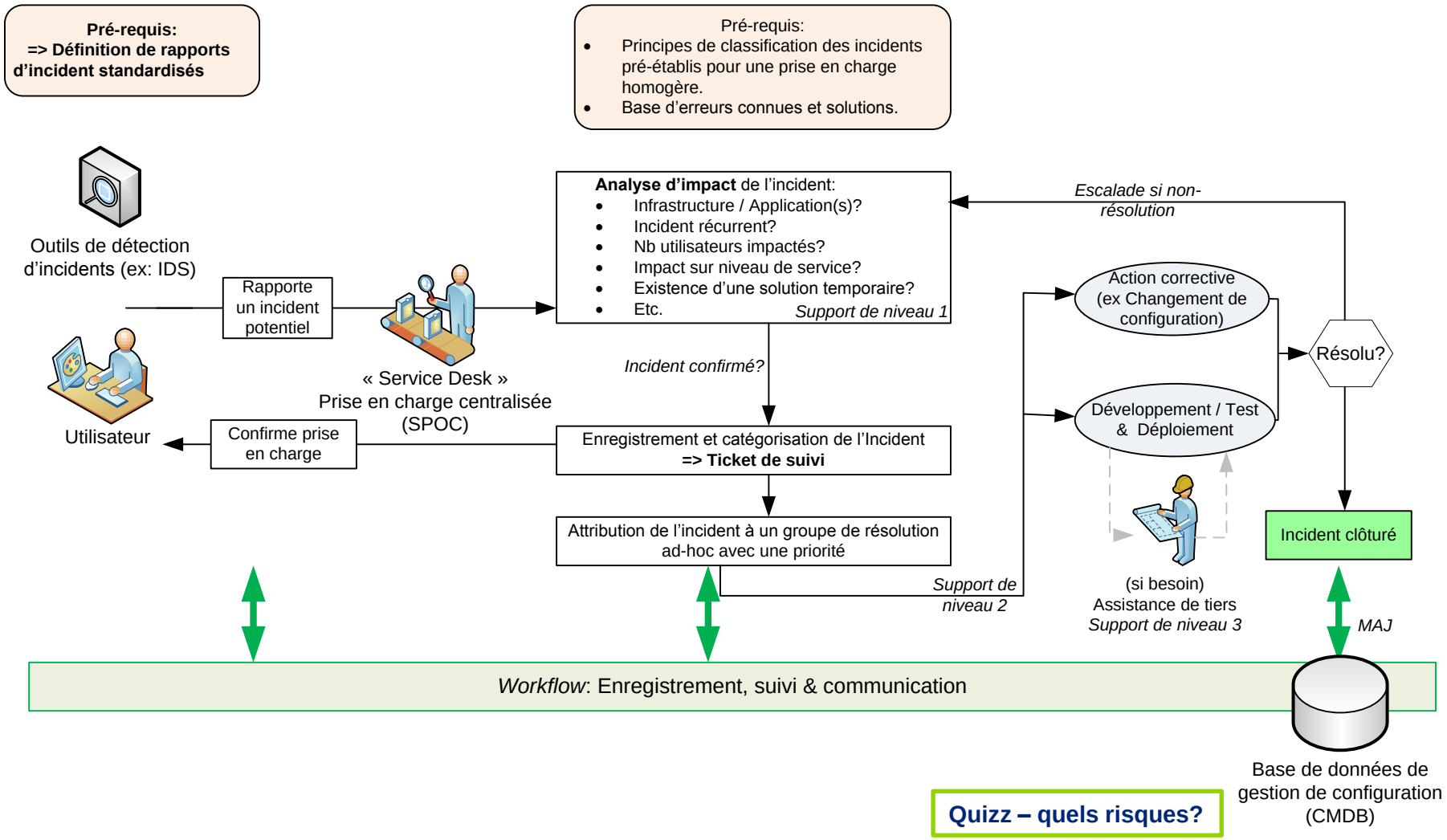
- Processus de gestion des incidents
- Processus de gestion des changements
- Processus de gestion des accès



Processus de gestion des incidents

Organisation de la sécurité

Exemple: Processus de gestion des incidents (simplifié) (1/3)



Quizz – quels risques?

Organisation de la sécurité

Risques et mesures de réduction: processus de gestion des incidents (2/3)

Exemples de facteurs de risques

- Détails insuffisants pour analyser l'incident
- Utilisateurs et équipes IT ne suivent pas le processus standard.
- Prioritisation inappropriée (insuffisante ou excessive) des incidents
- Nombre d'acteurs prenant part à la résolution et inder-dépendances
- Service Desk monopolisé par des incidents récurrents
- Incident clôturé mais non-résolu
- Formation insuffisante des équipes de support (ex: en cas de rotation de personnel)

Etc.

Exemples de mesures de réduction des risques

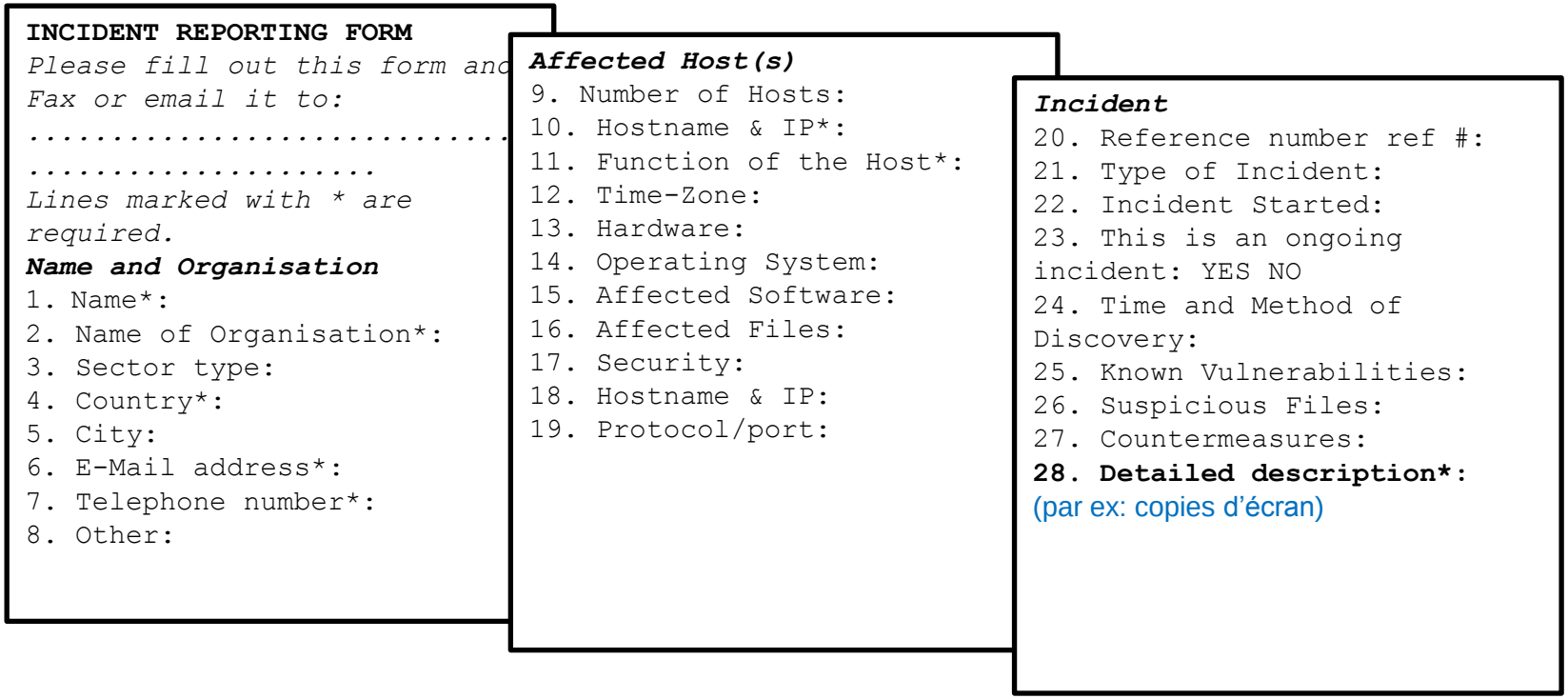
- Formulaires standardisés de rapports d'incidents
  Par ex: Modèles de l'ENISA
- Point de contact unique pour l'assistance utilisateur (« SPOC »).
- Principes de classification des incidents pré-établis et non-ambigüs pour assurer une prioritisation homogène.
- Incidents récurrents -> analyse des causes sous-jacentes (« Problem Management »)
- Définition d'un « propriétaire » pour chaque incident
- Clôture de l'incident par l'utilisateur
- Base de connaissance pour les incidents connus

Etc.

Organisation de la sécurité

Risques et mesures de réduction: processus de gestion des incidents (3/3)

Exemples de formulaires standardisés de rapports d'incidents:



INCIDENT REPORTING FORM
Please fill out this form and
Fax or email it to:
.....
.....
*Lines marked with * are required.*

Name and Organisation
1. Name*:
2. Name of Organisation*:
3. Sector type:
4. Country*:
5. City:
6. E-Mail address*:
7. Telephone number*:
8. Other:

Affected Host(s)
9. Number of Hosts:
10. Hostname & IP*:
11. Function of the Host*:
12. Time-Zone:
13. Hardware:
14. Operating System:
15. Affected Software:
16. Affected Files:
17. Security:
18. Hostname & IP:
19. Protocol/port:

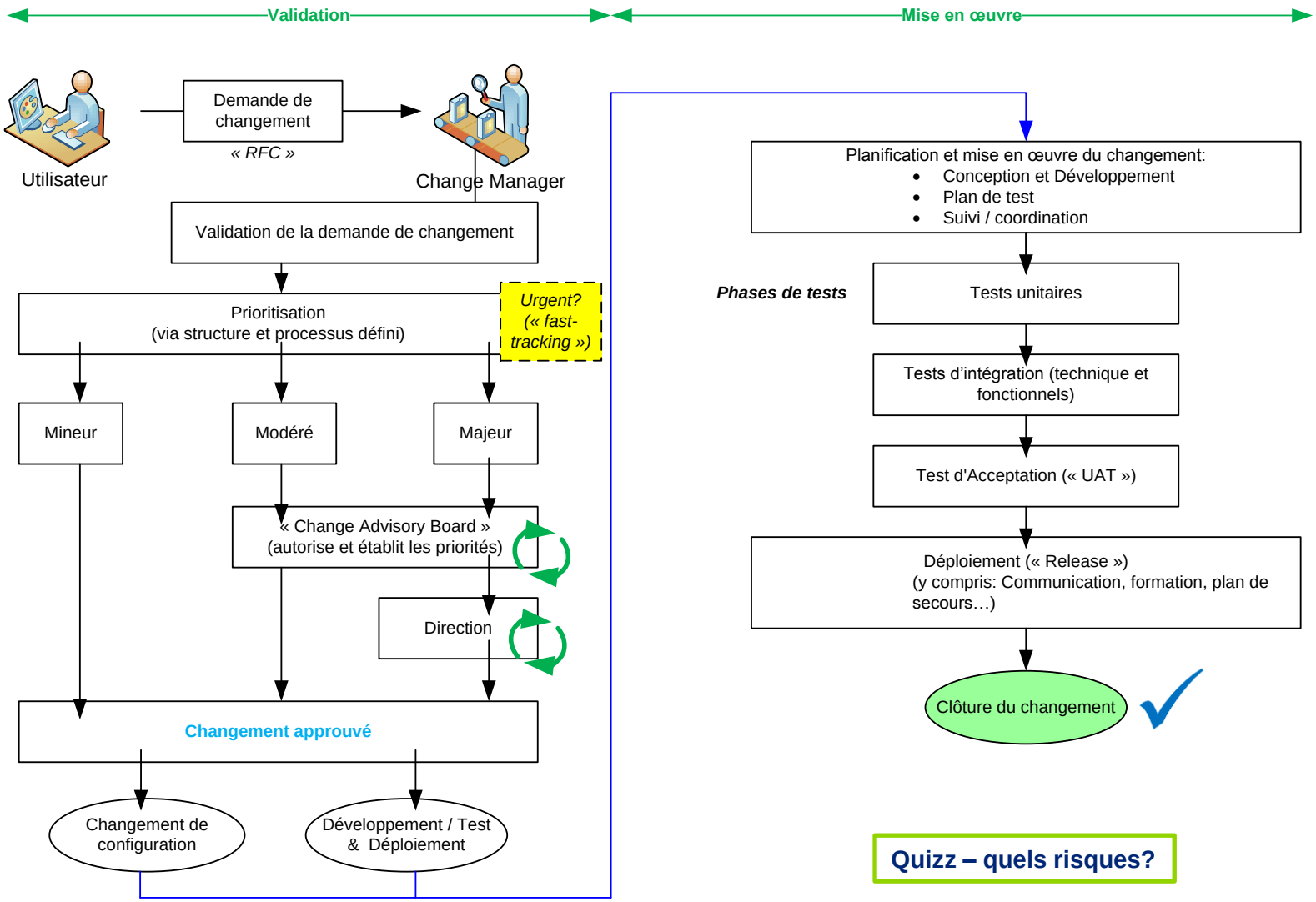
Incident
20. Reference number ref #:
21. Type of Incident:
22. Incident Started:
23. This is an ongoing incident: YES NO
24. Time and Method of Discovery:
25. Known Vulnerabilities:
26. Suspicious Files:
27. Countermeasures:
28. Detailed description*:
(par ex: copies d'écran)

Source: ENISA - http://www.enisa.europa.eu/activities/cert/support/incident-management

Processus de gestion des changements

Organisation de la sécurité

Exemple: Processus de gestion des changements (simplifié)

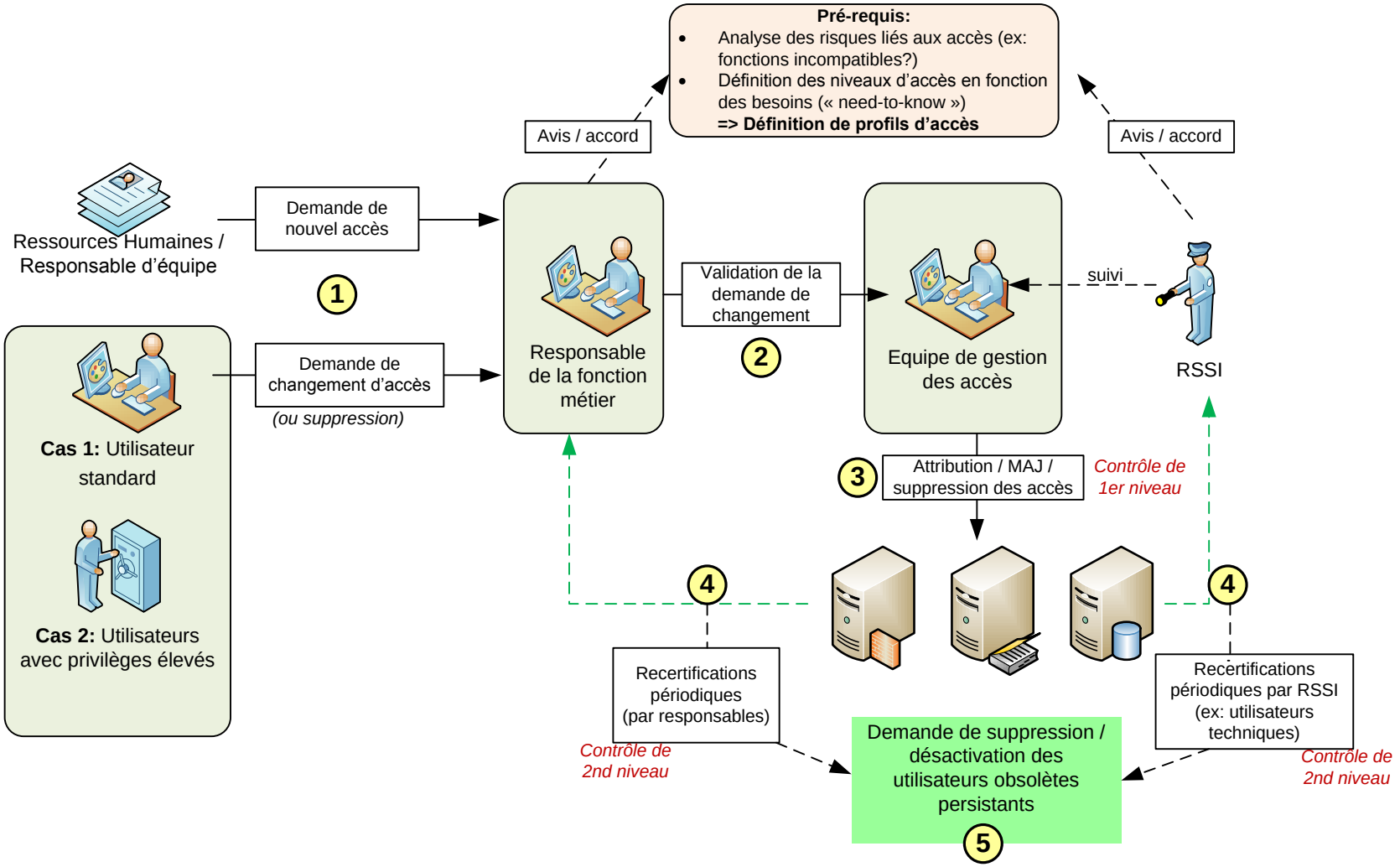


Quizz – quels risques?

Processus de gestion des accès

Organisation de la sécurité

Exemple: Processus standard de gestion des accès (simplifié) (1/2)



Quizz – quels risques?

Organisation de la sécurité

Risques: processus standard de gestion des accès (2/2)

Exemples de facteurs de risques

- Validité des demandes d'accès?
- Accès non-standardisés / non-uniformes pour un même besoin?
- Erreurs opérationnelles dans la mise en œuvre?
- Gestion des accès temporaires / de personnel externe ou intérimaire?
- Absence de demande de suppression en cas de départ?
- Suppression des accès dans les temps?
- Recertification effectuée mais actions correctrices non réalisées?

Etc.

Exemples de mesures de réduction des risques

- Habilitations à autoriser les accès formellement définies. Authentification *raisonnable* des demandes
- Formulaires standardisés de gestion des accès
- Contrôle des 4-yeux (sur fonctions sensibles, ex: accès aux applications de paiement)
- Analyse des risques & profils à droits réduits pour externes / personnel temporaire
- Accès temporaires avec date d'expiration pré-définie / recertification
- Sensibilitation / RSSI proactif

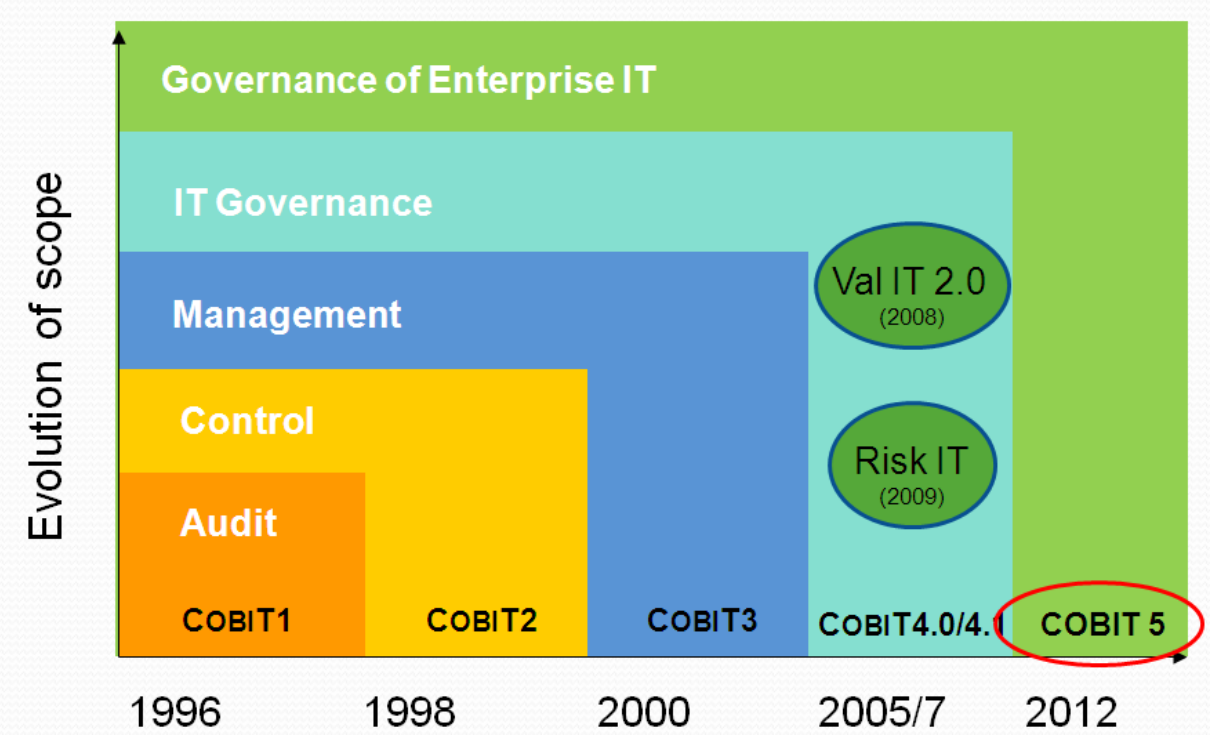
Etc.

IV) Cadres de référence: modèle et standards

- CobiT
- ISO/IEC 27001:2005 et 27002:2005
- Modèles de maturité

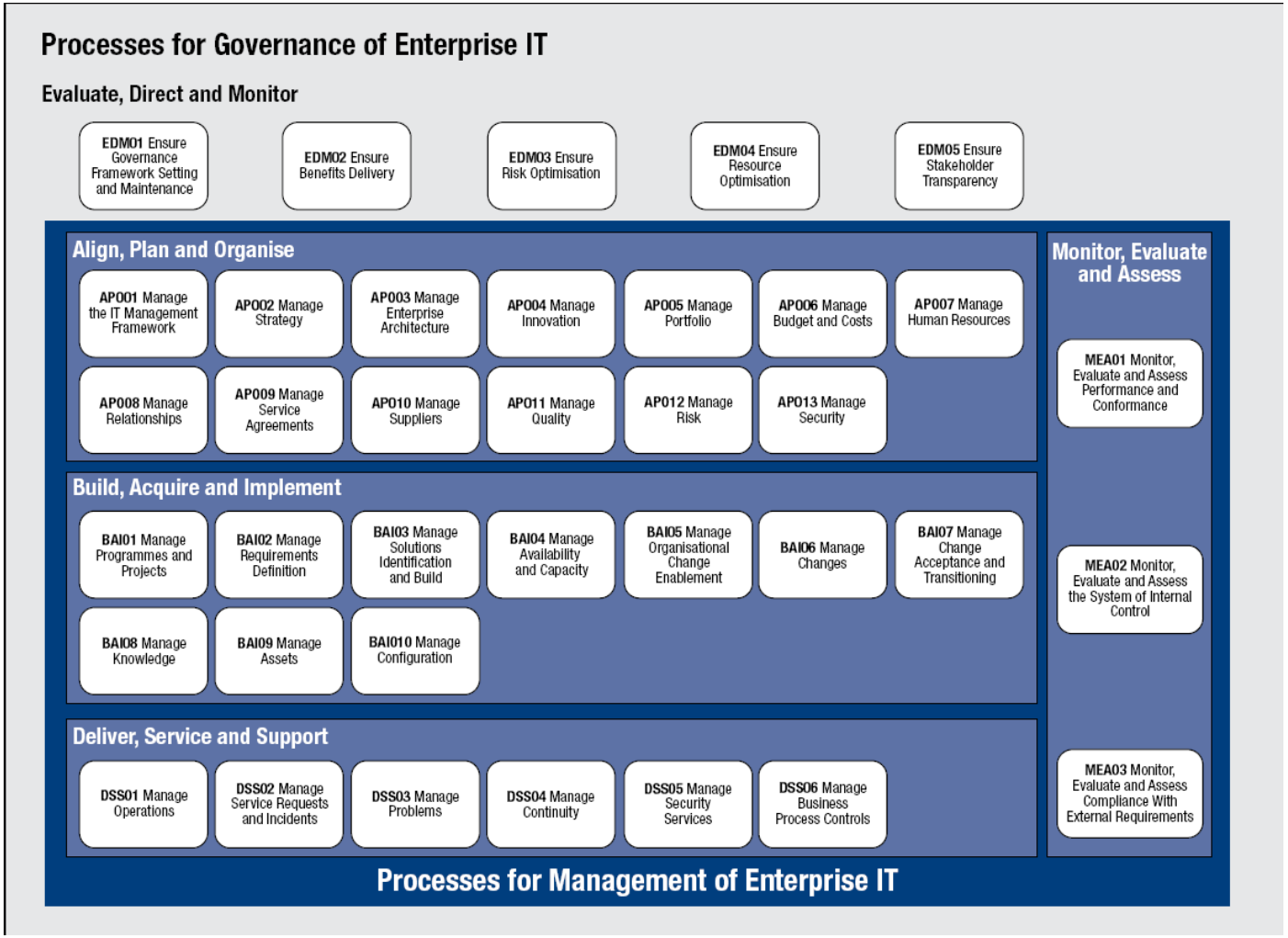
Cadres de référence: modèle et standards
CobiT - gouvernance des systèmes d'information

- **Control Objectives for Information and related Technology** (Objectifs de contrôle de l'Information et des Technologies Associées)
  - **Référentiel orienté Gouvernance des S.I.,** publié par l'ISACA
  - **Ensemble de bonne pratiques, orienté processus et Gouvernance**



Cadres de référence: modèle et standards
CobiT - gouvernance des systèmes d'information

- **Orienté autour de 4 étapes et 34 processus,** génériques et applicables à toute organisation ou entreprise.



Exemple

Cadres de référence: modèle et standards

ISO/IEC 27001:2005 - norme de gestion de sécurité de l'information

Refonte effectuée fin 2013

- Référentiel international de bonnes pratiques pour la gestion de la sécurité de l'information, publié en octobre 2005 par l'ISO.
- S'adresse à tous les types d'Organismes (toutes tailles, tous types d'activité). Pas d'obligation sur les méthodes. Possibilité de se faire certifier par un auditeur agréé (non-obligatoire).
- Décrit des exigences génériques (mais exhaustives) pour mettre en place un Système de Gestion de la Sécurité de l'information (« ISMS »):
  - 11 Domaines et 133 mesures de sécurité (refonte en 2013: 14 Domaines et 114 mesures de sécurité)
  - A pour objectif d'initier un processus d'**amélioration continue** de la sécurité (« PLAN, DO, CHECK, ACT »).

A.9 Physical and environmental security		
A.9.1 Secure areas		
Objective: To prevent unauthorized physical access, damage and interference to the organization's premises and information.		
A.9.1.1	Physical security perimeter	*Control* Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities.
A.9.1.2	Physical entry controls	*Control* Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
A.9.1.3	Securing offices, rooms and facilities	*Control* Physical security for offices, rooms, and facilities shall be designed and applied.
A.9.1.4	Protecting against external and environmental threats	*Control* Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied.

Domaine

Objectif de contrôle (générique)

Mesures de sécurité (génériques)

Cadres de référence: modèle et standards

ISO/IEC 27002:2005 – code de bonnes pratiques pour la gestion de la sécurité de l'information

- Complément de la norme ISO/IEC 27001/2005: guide pratique qui fournit des centaines de contrôles potentiels et mécanismes de contrôle pouvant être mis en place.

9.1.2 Physical entry controls

Control

Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

Implementation guidance

The following guidelines should be considered:

a) the date and time of entry and departure of visitors should be recorded, and all visitors should be supervised unless their access has been previously approved; they should only be granted access for specific, authorized purposes and should be issued with instructions on the security requirements of the area and on emergency procedures.

b) access to areas where sensitive information is processed or stored should be controlled and restricted to authorized persons only; authentication controls, e.g. access control card plus PIN, should be used to authorize and validate all access; an audit trail of all access should be securely maintained;

c) all employees, contractors and third party users and all visitors should be required to wear some form of visible identification and should immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification;

d) third party support service personnel should be granted restricted access to secure areas or sensitive information processing facilities only when required; this access should be authorized and monitored;

e) access rights to secure areas should be regularly reviewed and updated, and revoked when necessary (see 8.3.3).

Cadres de référence: modèle et standards
Référentiels utilisés pour la formalisation de la PSI

- **Quelques statistiques (2018):**(entreprises de plus de 100 salariés)

Bases sur lesquelles repose le pilotage de la sécurité de l'information	
Une ou plusieurs normes (ISO ou autre) et plus particulièrement :	**29%**
ISO 27001 et 27002	23%
LPM	1%
PCI-DSS	2%
Autre	6%
La Politique de sécurité interne	**24%**
Le management des risques, et en s'appuyant sur un référentiel :	**7%**
ISO 27005	1%
Méhari	1%
Ebios	2%
Autre	4%
Le management des incidents	**2%**
Bases de pilotage de la sécurité différentes ou non définies	**48%**

CLUSIF: 48% des entreprises « ont entrepris nombre d'actions de sécurité, sans avoir défini de système de pilotage », « ces actions découlent de bonnes pratiques communément reconnues, de mesures évidentes à mettre en œuvre après avoir identifié certains risques, ou de toute autre cause ».

Source: CLUSIF – Rapport 2018

Cadres de référence: modèle et standards
ISO 9001 / CMMI / CobiT CMM – modèles de maturité

- Modèles de mesure de la maturité des processus informatiques.
  - Orientés processus
  - Supportent une approche d'amélioration continue.

- Applicables à différents niveaux d'une organisation (équipe, département, société)

  • **CMMI** -> Orienté développement et maintenance logicielle. Evaluation possible par un évaluateur certifié (supervise une équipe d'évaluation interne et externe).

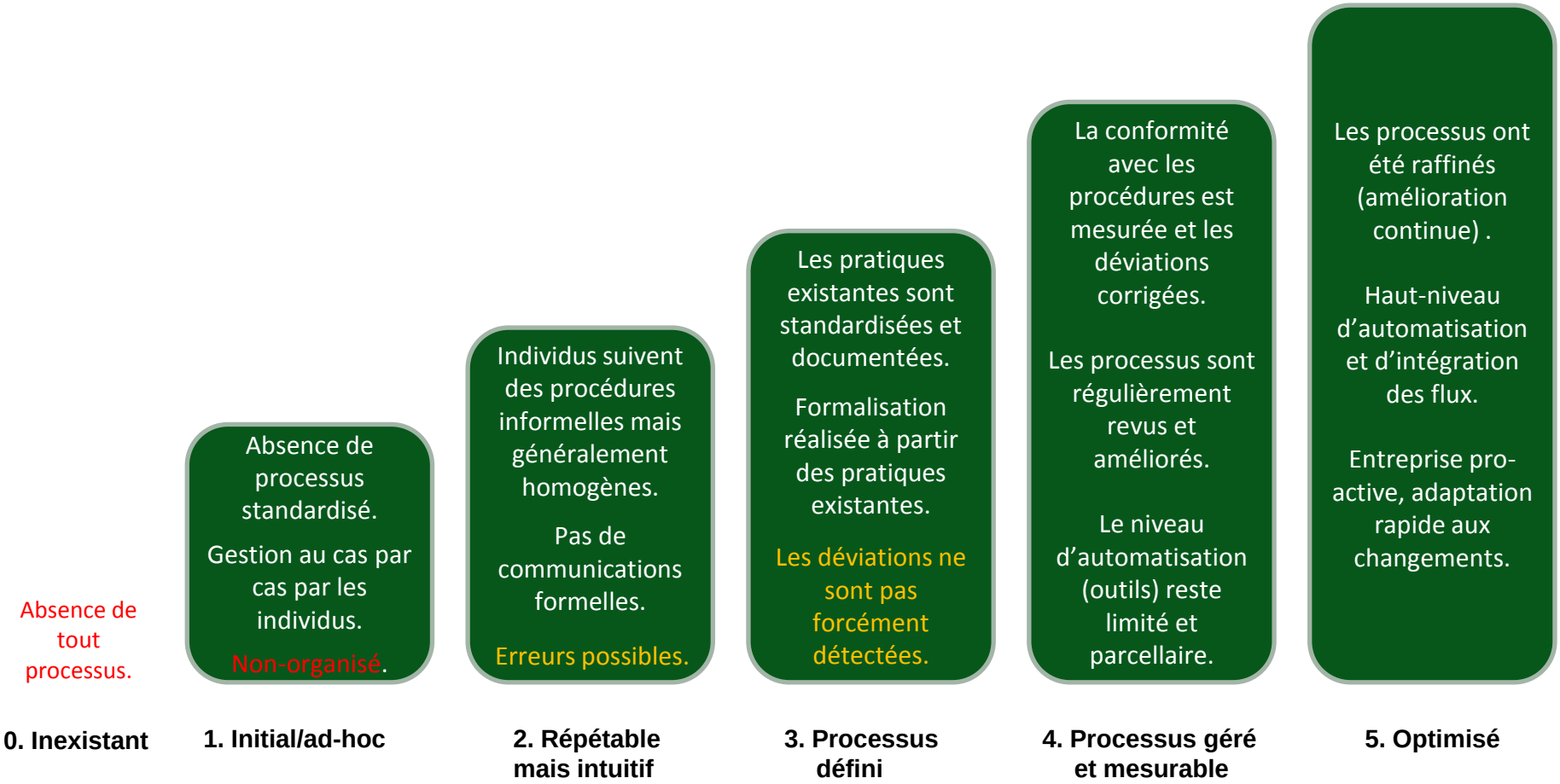
  • **ISO 9001** -> Norme internationale, applicable à l'ensemble des activités d'une organisation. (Possibilité de certification par un auditeur habilité).

  • **CobiT CMM** -> Approche de haut-niveau centrée sur la stratégie et le « profiling » des processus informatiques (-> outil de 'benchmarking', non-certifiant).

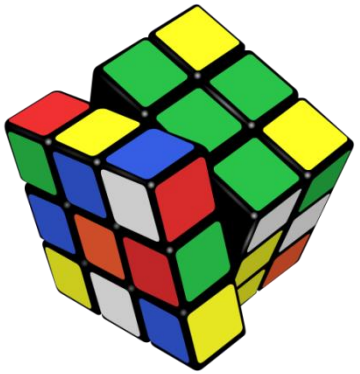
- En pratique:
  - ISO 9001 supporte généralement une démarche de certification.
  - CMMI supporte plutôt une démarche d'amélioration interne (liste de forces et faiblesses), orientée développement logiciel.
  - CobiT CMM a pour but de permettre une meilleure compréhension des processus de gestion du S.I.: benchmarking, analyses d'écart et plans d'améliorations.

Cadres de référence: modèle et standards
CobiT CMM – modèle de maturité

- Niveaux de maturité des processus informatiques (**CobiT CMM**):

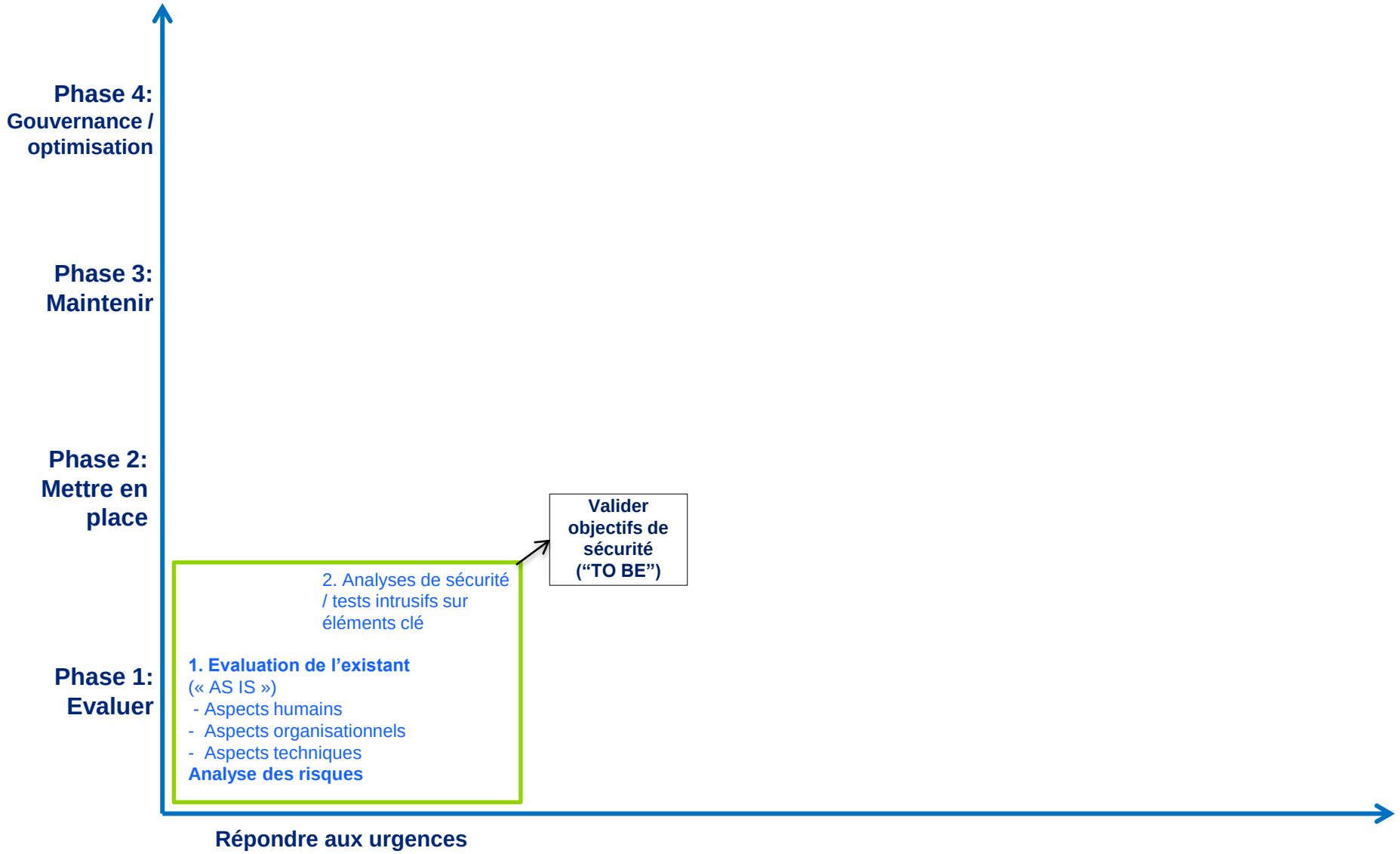


V) Exemple: modèle type pour la mise en place d'une stratégie de sécurité



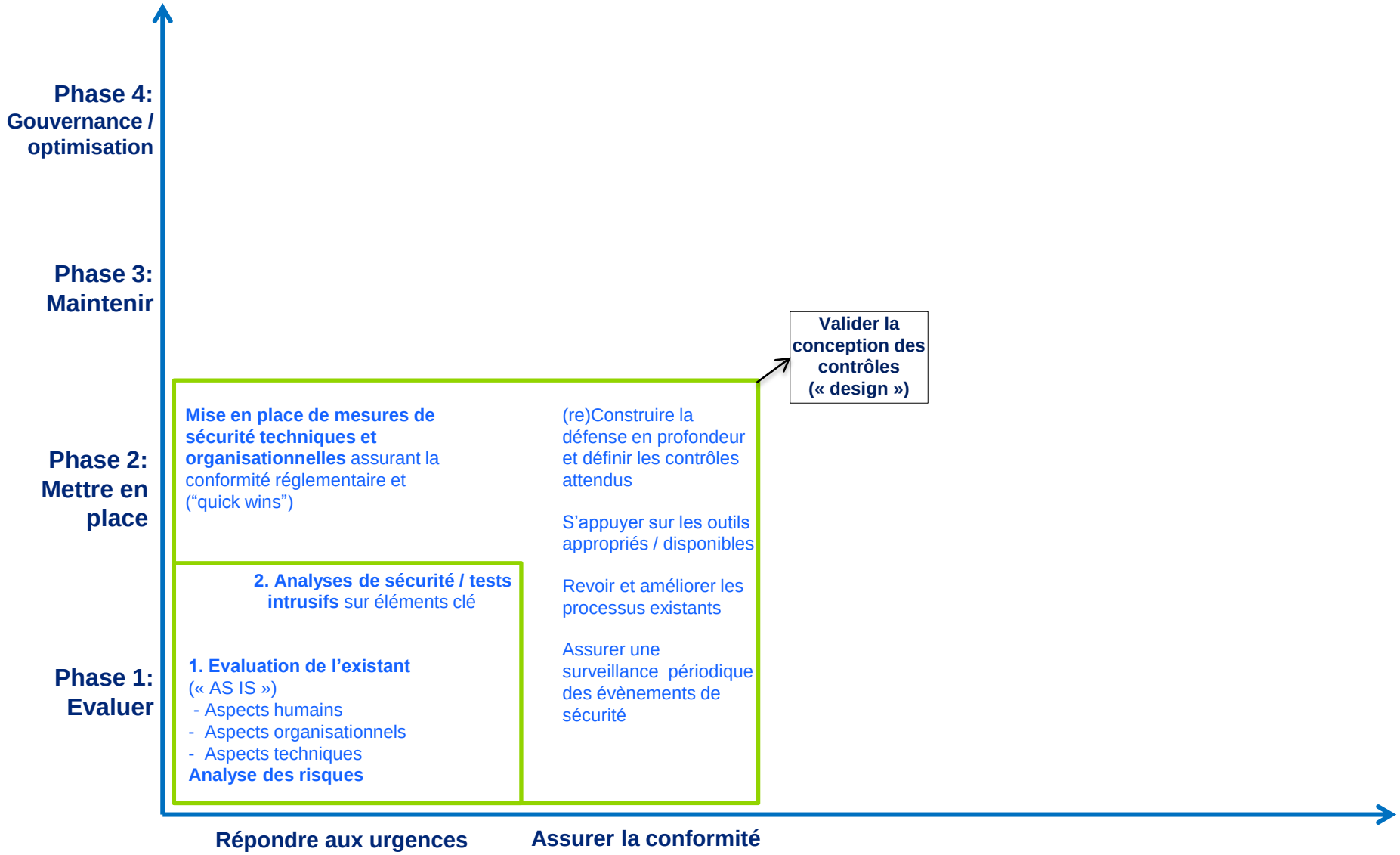
Exemple: modèle type pour la mise en place d'une stratégie de sécurité

Phase 1 – évaluation de l'existant (« AS IS »)



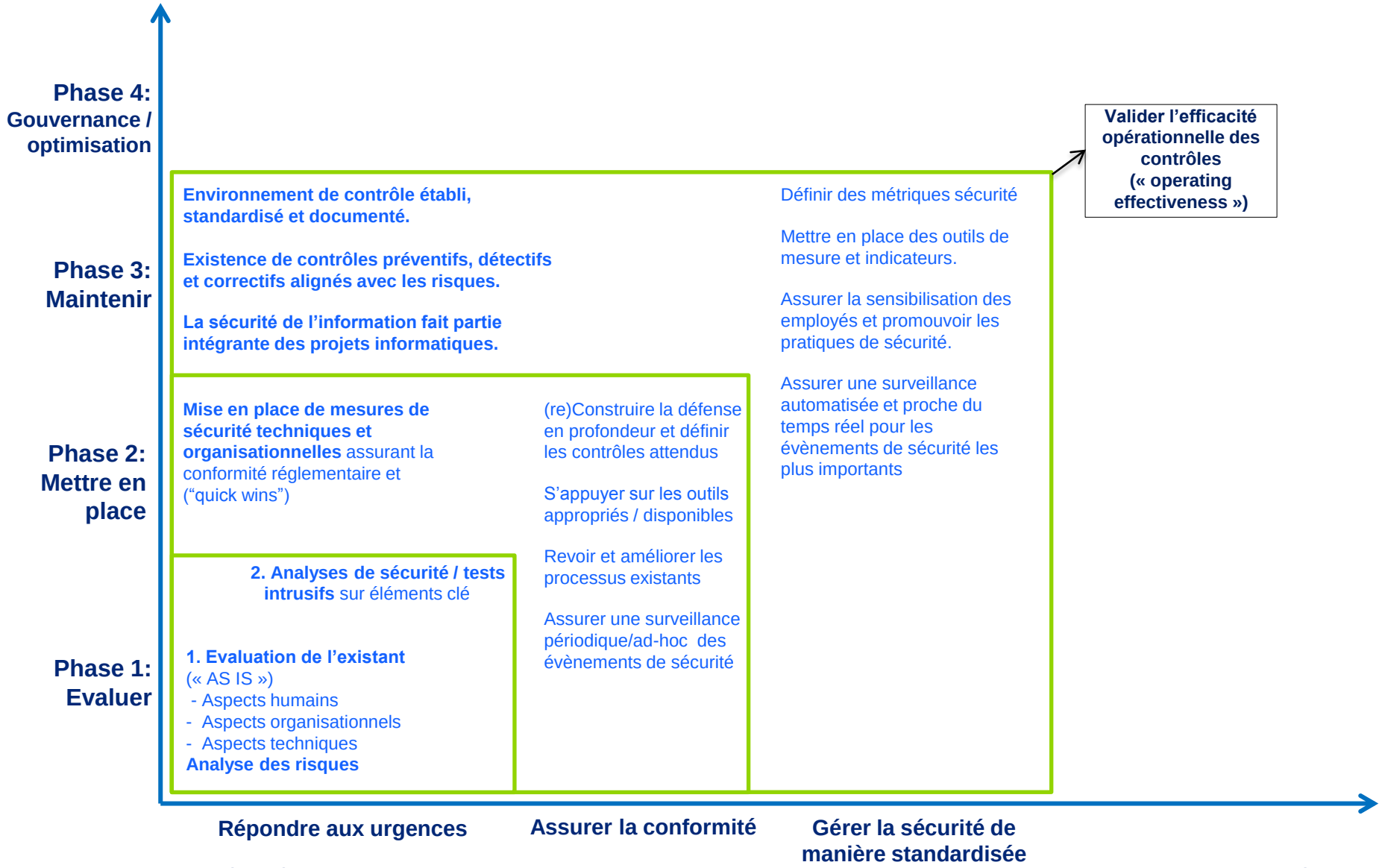
Exemple: modèle type pour la mise en place d'une stratégie de sécurité

Phase 2 – mise en place de mesures de sécurité alignées sur les risques



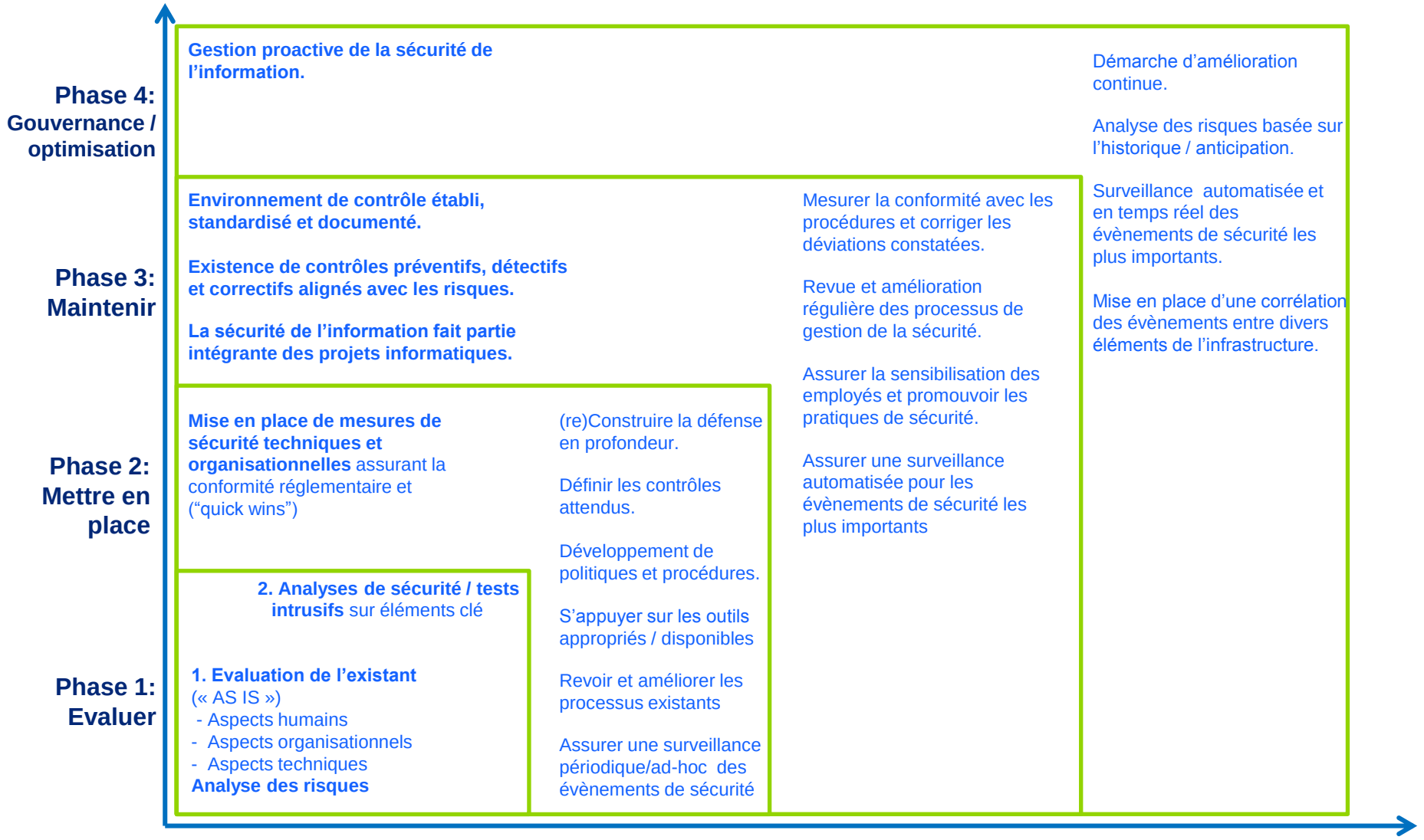
Exemple: modèle type pour la mise en place d'une stratégie de sécurité

Phase 3 – gestion de l'environnement de contrôle



Exemple: modèle type pour la mise en place d'une stratégie de sécurité

Phase 4 – gouvernance et optimisation de l'environnement de contrôle



Questions?