METZ - 15/12/09

AGENDA :

10h00 - 10h15 : Accueil - Café

10h15 - 11h30 : Intervention d'un expert sur COBIT/Val IT/ITIL & ISO27001 (Jean-Pierre Radoux - ALTRAN

11h30 - 12h30 : Intervention sur ISO 27005 (Thierry RAMARD - AGERIS)

12h30 - 15h00 : Pause déjeuner – Promenade fluviale sur la Moselle

15h15 – 16h30 : Tables rondes

Table ronde n° 1 : Plan de Continuité d'Activité (PCA)

Table ronde n° 2 : L'avenir de la gouvernance IT (ISACA vs ISO)

16h30 - 17h00 : Questions diverses – fonctionnement du CLUSIR- EST

Norme ISO / IEC 27005

METZ - 15/12/09

Thierry RAMARD

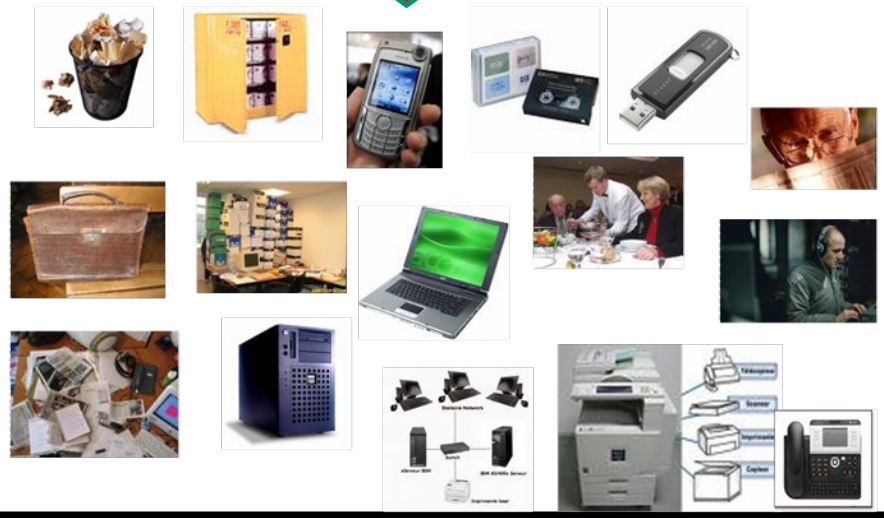
- Rappel général sur les concepts généraux de la gestion des risques
- Présentation générale de la norme ISO 27005
- Approche et contenu de la norme

Apports de dématérialisation
(productivité, efficacité, qualité)

=

Organisation et système d'information parfaitement maîtrisés et sécurisés

dématérialisation



CLUSIR EST

Norme ISO / IEC 27005

Apports de

(pr

sy

pa

Les exemples de perte de contrôle des informations sont nombreux

Données personnelles : débâcle sécuritaire en Angleterre

Banque, numéro de SECU, tout y passe

Le *Times Online* vient de révéler en Angleterre ce qui pourrait être la plus grave affaire de sécurité informatique connue, peu de temps après la perte de deux disques contenant les informations bancaires de 25 millions de citoyens britanniques par le gouvernement anglais.

Toutes les informations bancaires, jusqu'aux codes de sécurité

Une clé USB secret-défense oubliée

L'armée suédoise a reconnu vendredi que l'un de ses membres avait oublié une clé USB contenant des documents classés secret-défense dans un ordinateur public de Stockholm. Selon le quotidien *Aftonbladet* qui a renvoyé la clé USB à l'armée après l'avoir reçue d'un expéditeur anonyme, elle avait été oubliée une bibliothèque publique. La clé USB comprenaient une analyse de la situation en Afghanistan ainsi qu'un rapport secret du renseignement américain.

RL 06/01/2008

Rédigée par Bruno Cormier le mardi 04 décembre 2007 à 15h41

La bourde du fisc donne des sueurs froides aux Britanniques

RL 24/11/2007

La perte par le fisc de données sensibles fait peser sur près de la moitié des Britanniques des risques accrus de vol d'identité et d'escroquerie bancaire.

Angleterre : dans le vieux PC vendu s… eBay, les données bancaires d'u… d'Anglais

Insolite, PC, banques, données bancaires

…mployé de GraphicData, une société d'archivage de données de la …Bank of Scotland (RBS) voulait se débarrasser de son vieil ordinateur.

…mme des millions d'individus, il a choisi eBay pour la vente.

…se à prix: 44 euros.

…vieil ordinateur a trouvé preneur.

…is l'acquéreur a eu la surprise de découvrir que le disque dur du PC contenait …données bancaires d'un million de clients de la RSB mais aussi de deux autres …nques anglaises, American Express et Nat West,

Fuite de données pour le groupe ESRA

Publié le 11-09-2008 à 13:41

Pub : Participez à des batailles na… …000 € sur Bigpoint.fr

Note des lecte…

…formations sensibles d'élèves appartenant à …udiovisuelle oubliées sur Internet.

…la protection de données privées découverte par ZATAZ.CO… …mations sensibles appartenant plusieurs milliers de lycéens, étu… …Français. Des identités, téléphones, courriels trouvés dans six ba… …laissées à l'abandon sur la toile par le groupe de l'Ecole Supérie… …alisation Audiovisuelle, un spécialiste dans les métiers de l'image et du son … pour les métiers du Cinéma et de l'audiovisuel. L'ISTS pour les métiers du … SUP'INFOGRAPH pour ceux du film d'animation 3D).

ZATAZ.COM a découvert, la semaine dernière, plusieurs fichiers qui n'auraient … du être disponible, sur la toile, avec un simple navigateur, sans protection, ni co… …nts textes, certains ayant des contenus datant de 2003, dans les… …le de trouver les noms, adresses, téléphones, courriels, form… …nvoyés par courriels, niveaux d'études, mots de passe, …

…ases de données, des informations envoyées par des lycéens, étu… …ouhaitant s'orienter vers les cursus proposés par l'ESRA. Contac… …l'école a mis une vingtaine de minutes à peine pour corriger son pro…

Données sensibles : la grande évasion

Le ministère britannique de l'Intérieur admet la perte des données personnelles relatives à tous les détenus et délinquants d'Angleterre et du Pays de Galles.

Il ne s'agit là que du dernier épisode en date d'une série de bourdes qui ont provoqué une véritable hémorragie de données sensibles au Royaume-Uni.

P.L. - 1a 22/06/2008 - 18h56

…une fuite de don… …abrique cachée dans un tableau Ex… …méros de Sécurité Sociale d'offi… …SAASC

…e appartenant à la base militaire …ort Lewis disparaissait, avec au moins … …vées et sensibles

…ossiers et photos appartenant au Mi-6, dans la mém… …un appareil photo numérique, vendue sur eBay…

L'opérateur T-Mobile admet la fuite de données sur 17 millions de clients

1 votes

voter

L'opérateur T-Mobile admet la fuite de données sur 17 millions de clients

soumis par ItNewsInfo 145 jours depuis via rss.feedsportal.com

L'opérateur mobile T-Mobile, filiale de Deutsche Telekom, a déclaré samedi dernier que des données personnelles sur 17 millions de clients ont été « perdues (...)

Le dossier top secret qui embarrasse Gordon Brown

3 enjeux sécurité pour l'entreprise

- **L'information est un actif de plus en plus sensible**
  ⇨ Assurer disponibilité, intégrité et confidentialité

- **Des menaces et des risques exposent l'entreprise à des dysfonctionnements majeurs des processus critiques**
  ⇨ Maîtriser et prévenir les risques

- **Les obligations légales et les responsabilités juridiques se précisent**
  ⇨ Respect des obligations et mise en conformité nécessaires

L'information doit être protégée de manière adéquate

Protéger l'information consiste à garantir :

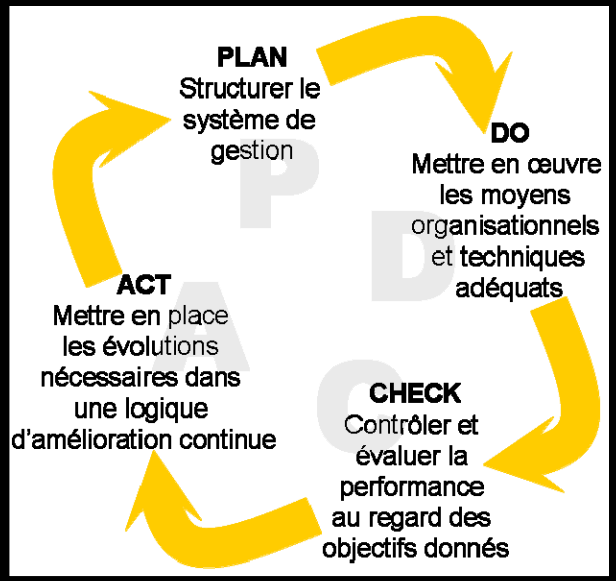
- **Sa Disponibilité**
  accessible en continu ; performance ; qualité
- **Son Intégrité**
  aucune altération ; exactitude ; exhaustivité
- **Sa Confidentialité**
  accès restreint ; classification
- **Sa Traçabilité**
  identification et analyse de tous les événements ; non-répudiation ; preuve

Mettre en œuvre un processus d'amélioration continue

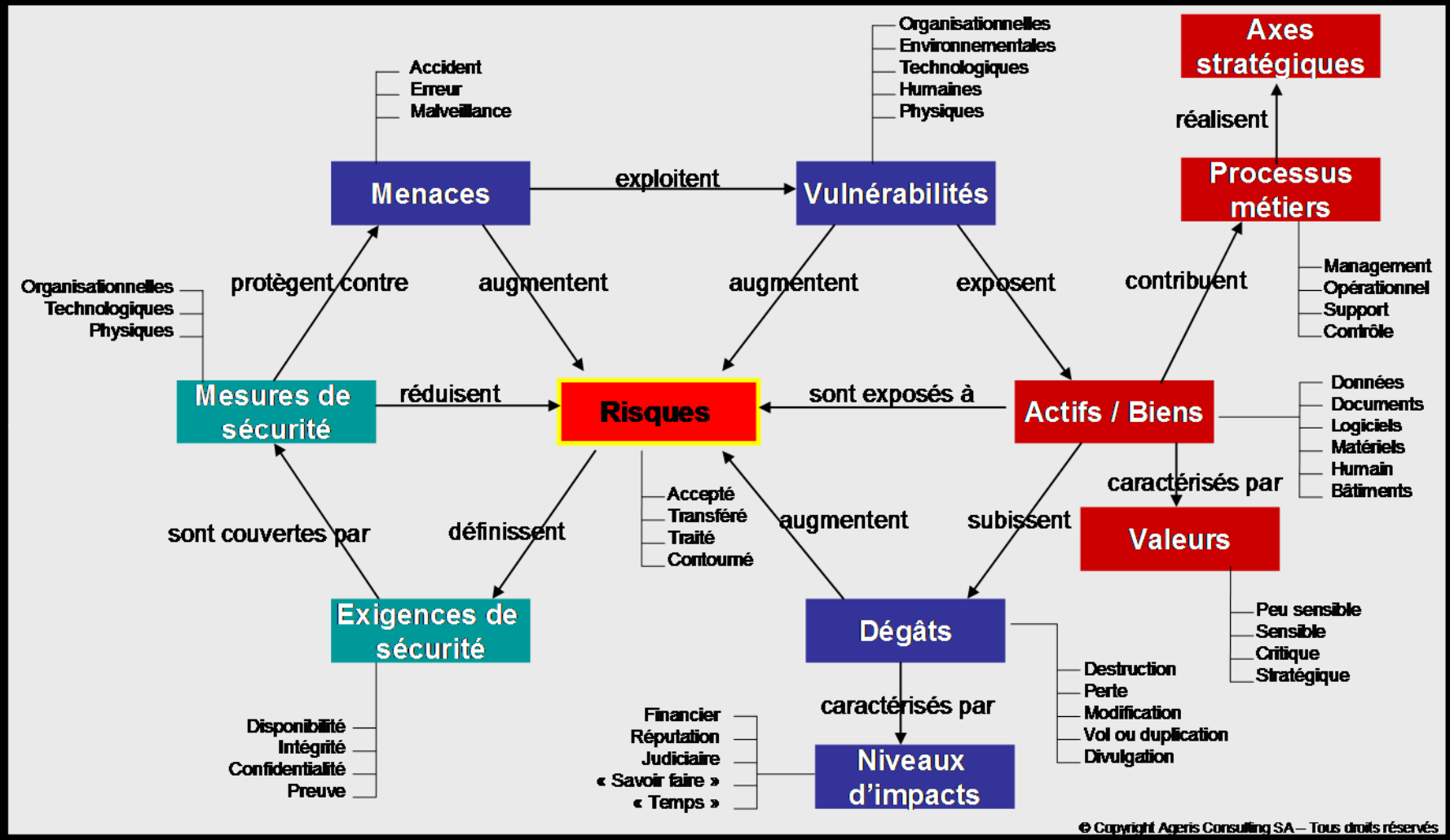
La norme ISO 27001 a pour objectif de proposer un modèle permettant de définir, d'implémenter, de maintenir, de piloter, d'auditer et de faire évoluer un système de management de la sécurité de l'information.

L'adoption de l'ISMS doit être une décision stratégique de l'organisation.

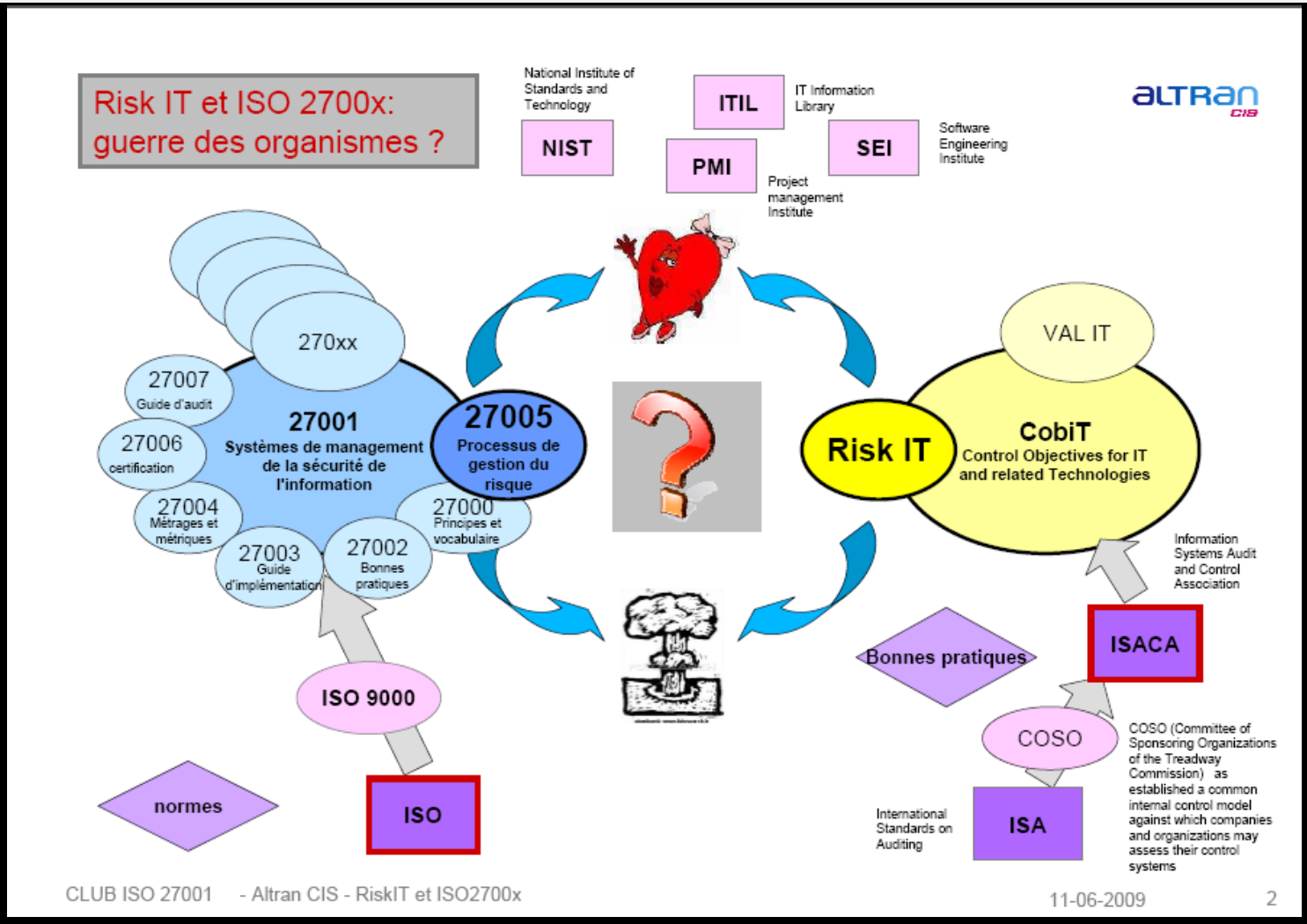
La norme adopte le modèle d'amélioration continue PDCA (Roue de Deming) et reprend les recommandations définies par l'OCDE pour introduire une culture de la sécurité.



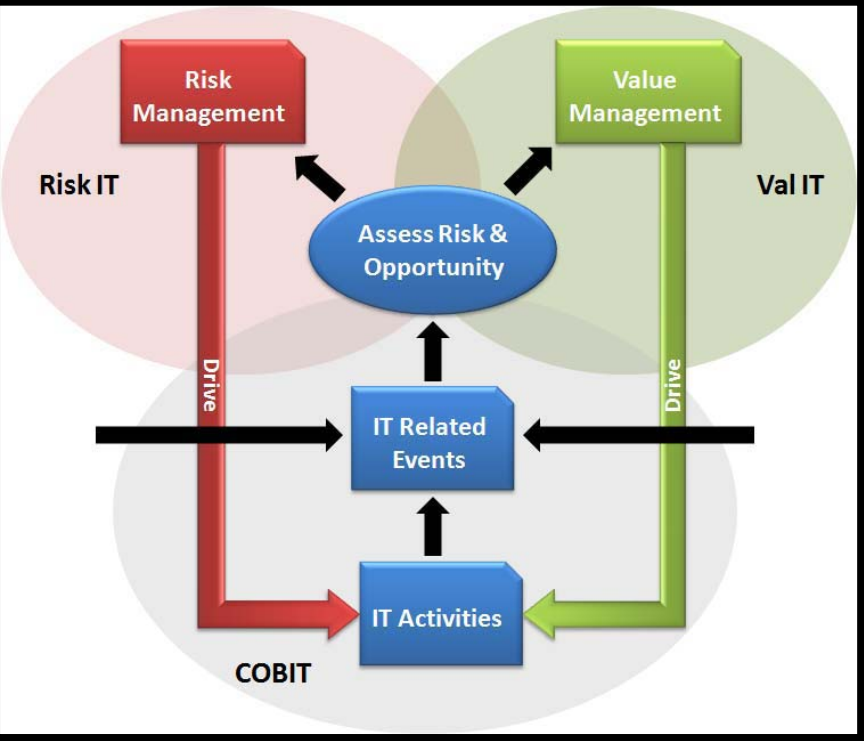
Rappel des concepts généraux de la gestion des risques



ISO vs ISA


Risk IT et ISO 2700x: guerre des organismes ?
National Institute of Standards and Technology
NIST
ITIL
IT Information Library
PMI
Project management Institute
SEI
Software Engineering Institute
ALTRAN CIS
270xx
27007 Guide d'audit
27006 certification
27004 Métrages et métriques
27003 Guide d'implémentation
27001 Systèmes de management de la sécurité de l'information
27005 Processus de gestion du risque
27000 Principes et vocabulaire
27002 Bonnes pratiques
ISO 9000
normes
ISO
VAL IT
Risk IT
CobiT Control Objectives for IT and related Technologies
Information Systems Audit and Control Association
ISACA
Bonnes pratiques
COSO
COSO (Committee of Sponsoring Organizations of the Treadway Commission) as established a common internal control model against which companies and organizations may assess their control systems
International Standards on Auditing
ISA

ISO vs ISA



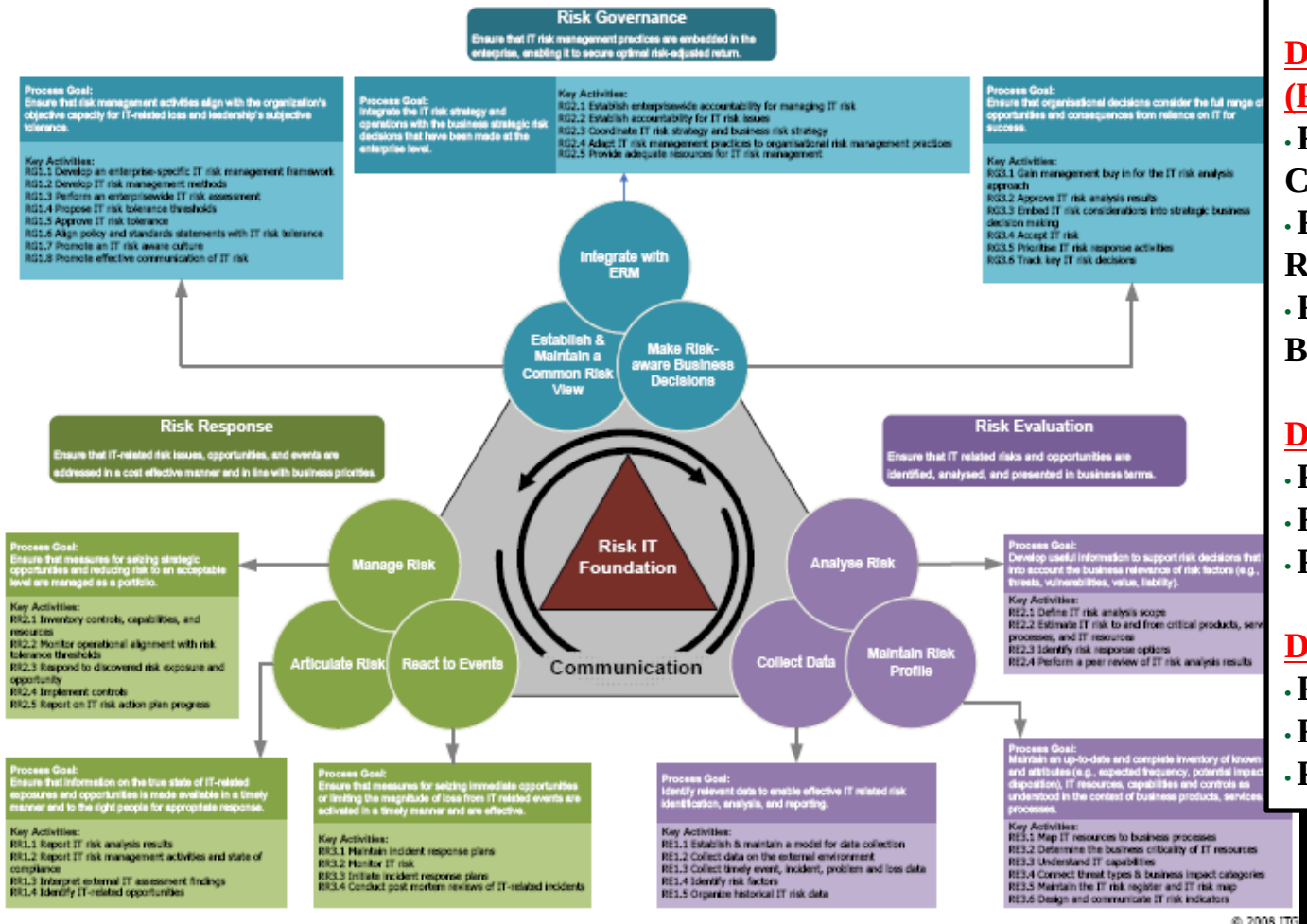
CobiT vient du monde de l'audit informatique et a pour objectif de s'assurer que l'informatique remplit le rôle qui lui a été assigné dans le développement de l'entreprise.

CobiT V4.1 décrit l'informatique en 4 domaines de 34 processus qui respectent la déclinaison : planifier, construire, opérer et surveiller. Chaque processus peut être évalué sur une échelle de maturité de 0 à 5. CobiT s'est imposé comme une description de référence de la gouvernance de l'informatique, un langage compréhensible par toutes les parties-prenantes et permet de construire facilement d'évaluer la performance globale de l'informatique.

De la notion initiale de contrôle, on est passé à l'évaluation plus précise de la valeur: Val IT et à la maîtrise des risques informatiques: Risk IT

Risk IT identifie trois domaines de trois processus essentiels chacun et 46 activités en tout

Figure 13—Risk IT Process Model Overview



The Risk IT Framework

Domain—Risk Governance (RG)

- RG1 Establish and Maintain a Common Risk View
- RG2 Integrate With Enterprise Risk Management (ERM)
- RG3 Make Risk-aware Business Decisions

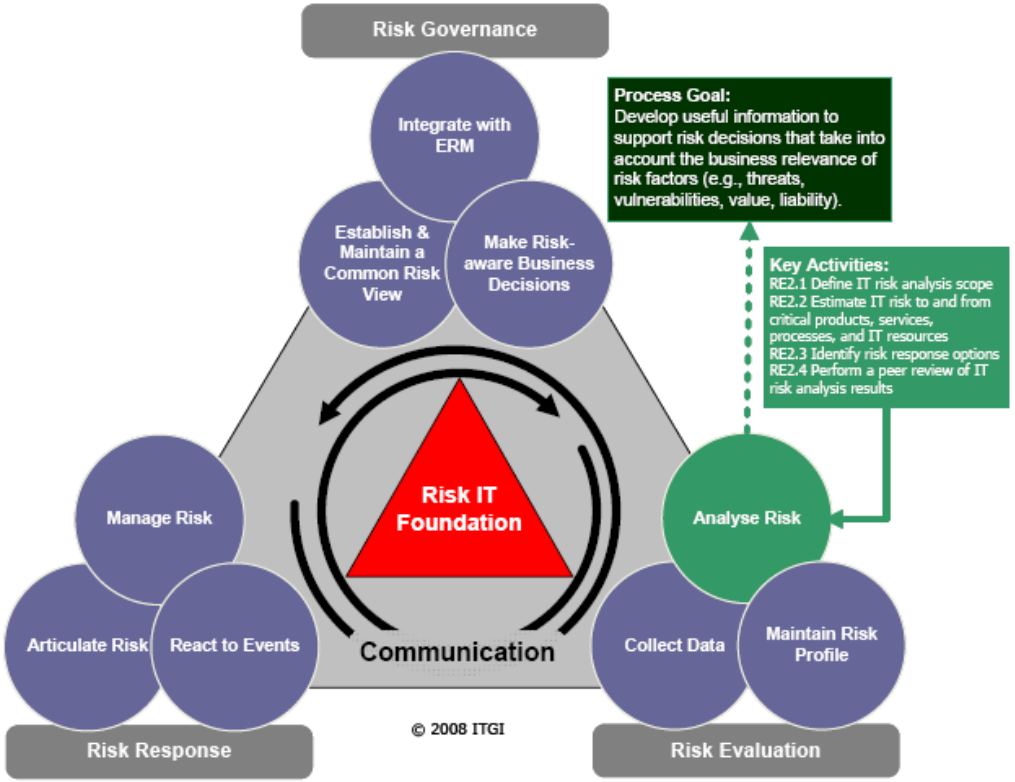
Domain—Risk Evaluation (RE)

- RE1 Collect Data
- RE2 Analyse Risk
- RE3 Maintain Risk Profile

Domain—Risk Response (RR)

- RR1 Articulate Risk
- RR2 Manage Risk
- RR3 React to Events

Figure 26—Process RE2 Analyse Risk



MANAGEMENT GUIDELINES—RE2

RACI Chart

Key Activities \ Roles	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
RE2.1 Define IT risk analysis scope.		I	R	C	I	C	A	R	C		C
RE2.2 Estimate IT risk to and from critical products, services, processes and IT resources.		I	R	C	C	I	A/R	R	R		C
RE2.3 Identify risk response options.			C	C	C	R	A	R	R		I
RE2.4 Perform a peer review of IT risk analysis results.			A/R				I		I		

A RACI chart identifies who is Responsible, Accountable, Consulted and/or Informed.

27005

emplate=_ContentManagement_ContentDisplay.pdf - Adobe Acrobat Standard

laires Outils Options avancées Fenêtre Aide

xporter Démarrer la réunion Protection Signature Révisions et commenta

75% Rechercher

PROCESS DETAIL

RE2 Analyse Risk

RE2.1 Define IT risk analysis scope.

Decide on the expected breadth and depth of risk analysis. Base the decision on the requirements of strategic decision makers (e.g., new products and services, new operating environments); risk focus areas identified through enterprise-wide IT risk assessment; or in response to indicators, triggers, or events (e.g., new or emerging threat populations). In addition, consider management's need for further examination of ongoing operations (e.g., line of business, product, service and process—individually or in combinations). From the risk profile, map in the established criticality of in-scope IT assets and triggers. Set the risk analysis scope after a final consideration of the criticality of assets, cost to analyse and potential overarching regulatory requirements.

From	Inputs
RG1.1	IT risk management framework
RG1.1	IT risk management methods
RG1.3	Risk analysis focus areas
RG3.3	Business decisions
RG3.3	Potential risk issues and opportunities
RG3.4, RE2.8, RE3.4	IT risk issues and business impacts
RE1.4, RE1.5	Risk factors
RE3.2	Business criticality of assets
RR2.2	Risk and control data
COBIT ME3	Cataloque of legal and regulatory requirements related to IT service delivery

To	Outputs
RE2.2	IT risk analysis scope

RE2.2 Estimate IT risk to and from critical products, services, processes and IT resources.

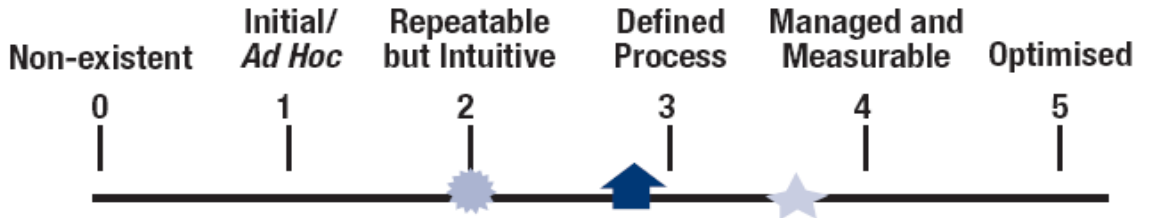
Identify threats against risk assets (i.e., the assets that fall within the scope of the risk analysis). Estimate the probable frequency of occurrence and magnitude of the business impact. Estimate the maximum amount of damage that could be suffered (e.g., a worst-case loss when specific risk factors converge). Across the scope of the risk analysis, consider scenarios of cascading and coincidental threat types (e.g., an external threat plus an internal accident). Based on the most probable scenarios, develop expectations for specific controls, capabilities and resources (CCR). Estimate the effect that known operational CCR will have on threats against highly ranked assets and targets. Partition CCR into the following categories: CCR deployed in line with expectations and with no known operating deficiencies; CCR deployed in line with expectations with known operating deficiencies (via other reviews); and CCR deployed beyond expectations with no known operating deficiencies. This third category of CCR may not be justified and could indicate opportunity for cost reduction while maintaining the same level of risk.

From	Inputs
RG1.2	IT risk management methods
RG1.5	IT risk tolerance thresholds
RE1.2, RE2.2	External environment data
RE1.4	Risk factors
RE1.5	Historical loss data
RE2.1	IT risk analysis scope
RE3.2	Relative ranking and classification of risk assets
RE3.2	Scope of expected controls
RE3.3	IT capability mappings
RR2.1, RR2.2	Control inventory mapped to IT risk statements
COBIT PO5	Enterprise IT control framework
*	Audit findings

To	Outputs
RE2.3	Risk analysis results (draft)
RE2.3	Risk exposures

Pour chaque domaine de risque informatique, il existe des modèles de maturité globaux et détaillés.
L'utilisation des modèles de maturité permet au management d'identifier:
- **les performances actuelles de l'entreprise**
- **les objectifs d'amélioration (p.ex. appétance pour le risque, style de gestion, capacité d'exposition au risque, ..)**

Les modèles détaillés sont construits autour des attributs suivants:
- **Sensibilisation et communication**
- **Responsabilités et imputabilité**
- **Définition des objectifs et mesures associées**
- **Politiques, standards et procédures**
- **Compétences et expertises**
- **Outils et automatisation**



LEGEND FOR SYMBOLS USED

- Enterprise current status
- Industry average
- Enterprise target

LEGEND FOR RANKINGS USED

0—Management processes are not applied at all.
1—Processes are *ad hoc* and disorganised.
2—Processes follow a regular pattern.
3—Processes are documented and communicated.
4—Processes are monitored and measured.
5—Good practices are followed and automated.

Exemple de Cadre légale et réglementaire

Premier ministre	Ministère du budget, des comptes publics et de la fonction publique
Direction Centrale de la Sécurité des Systèmes d'information	Direction Générale de la Modernisation de l'Etat

Administration Electronique :

Référentiel Général de Sécurité

La loi n° 2004-1343 du 9 décembre 2004 - Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives (ci-après désignée [Ordonnance]).

2.2.3 - Gérer les risques SSI

La démarche générale consiste principalement à :

- établir le contexte (délimiter et décrire la situation) ;
- apprécier les risques (les mettre en évidence et les hiérarchiser) ;
- traiter les risques (réduire, transférer, éviter les risques, ou accepter de les prendre).

Cette démarche, dont un cadre théorique est proposé par l'[ISO27005], peut être conduite de manière allégée dans les cas simples ou très détaillée si le système d'information est complexe et les enjeux élevés.

La mise en œuvre pratique de l'[ISO27005] doit s'appuyer sur les explications et les outils fournis dans les méthodes de gestion des risques telles que [EBIOS] (Expression des Besoins et Identification des Objectifs de Sécurité).

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

GROUPEMENT D'INTÉRÊT PUBLIC DOSSIER MÉDICAL PERSONNEL

Demande d'agrément pour l'hébergement de données médicales instauré par le décret n° 2006-6 du 4 janvier 2006

R. 1111-14 4 d Les modalités retenues pour l'évaluation périodique des risques et l'audit des mesures de protection mises en place afin de garantir la sécurité des données et en vue d'apporter les modifications nécessaires en cas de détection de défaillances ;

La norme ISO 27005

La présente Norme internationale **contient des lignes directrices relatives à la gestion de risque en sécurité de l'information** dans une organisation qui viennent, notamment, en appui des exigences d'un SMSI tel qu'il est défini dans l'ISO/CEI 27001.

Cependant, la présente Norme internationale **ne fournit aucune méthodologie spécifique** à la gestion de risque en sécurité de l'information.
Il est du ressort de chaque organisation de définir son approche de la gestion de risque, en fonction, par exemple, du périmètre du SMSI, de l'existant dans le domaine de la gestion de risques, ou encore du secteur industriel. **Plusieurs méthodologies existantes peuvent être utilisées en cohérence avec le cadre décrit** dans la présente Norme internationale pour appliquer les exigences du SMSI.

La présente Norme internationale s'adresse **aux responsables et aux personnels concernés par la gestion de risque** en sécurité de l'information au sein d'une organisation et, le cas échéant, aux tiers prenant part à ces activités.

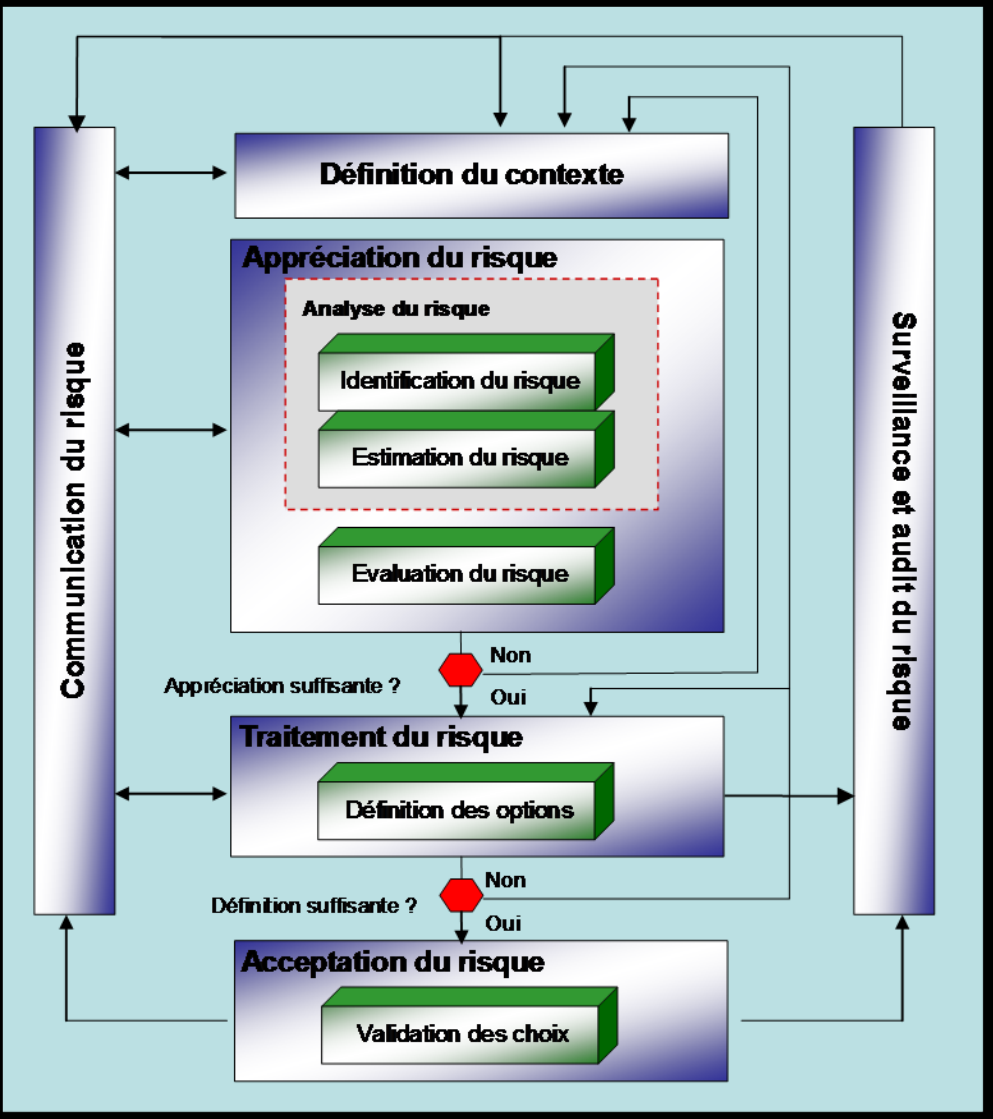
afnor NORMALISATION

Avant-projet de norme soumis à enquête probatoire jusqu'au : 15 octobre 2009

L'ISO/CEI 27005 a été élaborée par le comité technique ISO/TC JTC1, *Technologies de l'information, sous-comité SC 27, Techniques de sécurité des TI.*

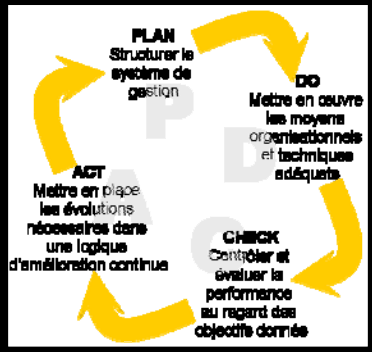
Cette première édition de l'ISO/CEI 27005 **annule et remplace l'ISO/CEI TR 13335-3:1998, et l'ISO/CEI TR 13335-4:2000,** dont elle constitue une révision technique.

La présente Norme internationale **est applicable à tous types d'organisations** (par exemple, les entreprises commerciales, les agences gouvernementales, les organisations à but non lucratif) qui ont l'intention de gérer des risques susceptibles de compromettre la sécurité de leurs informations.



Démarche proposée par la norme

Processus SMSI	Processus de gestion du risque en sécurité de l'information
Planifier	Etablissement du contexte Appréciation du risque Elaboration du plan de traitement du risque Acceptation du risque
Déployer	Mise en œuvre du plan de traitement du risque
Contrôler	Surveillance et réexamen continus des risques
Agir	Maintien et amélioration du processus de gestion du risque en sécurité de l'information



7 Etablissement du contexte

7.1 Considérations générales

Eléments d'entrée : Toutes les informations relatives à l'organisme permettant l'établissement du contexte de la gestion du risque en sécurité de l'information.

Action : Il convient d'établir le contexte de la gestion du risque en sécurité de l'information, ce qui implique de déterminer les critères de base nécessaires à la gestion du risque en sécurité de l'information (7.2), de définir le domaine d'application et les limites (7.3), et d'établir une organisation adaptée au fonctionnement de la gestion du risque en sécurité de l'information (7.4).

7.2 Définition des Critères de base
Selon le domaine d'application et les objectifs de la gestion du risque, différentes approches peuvent s'appliquer. L'approche peut également être différente pour chaque itération.

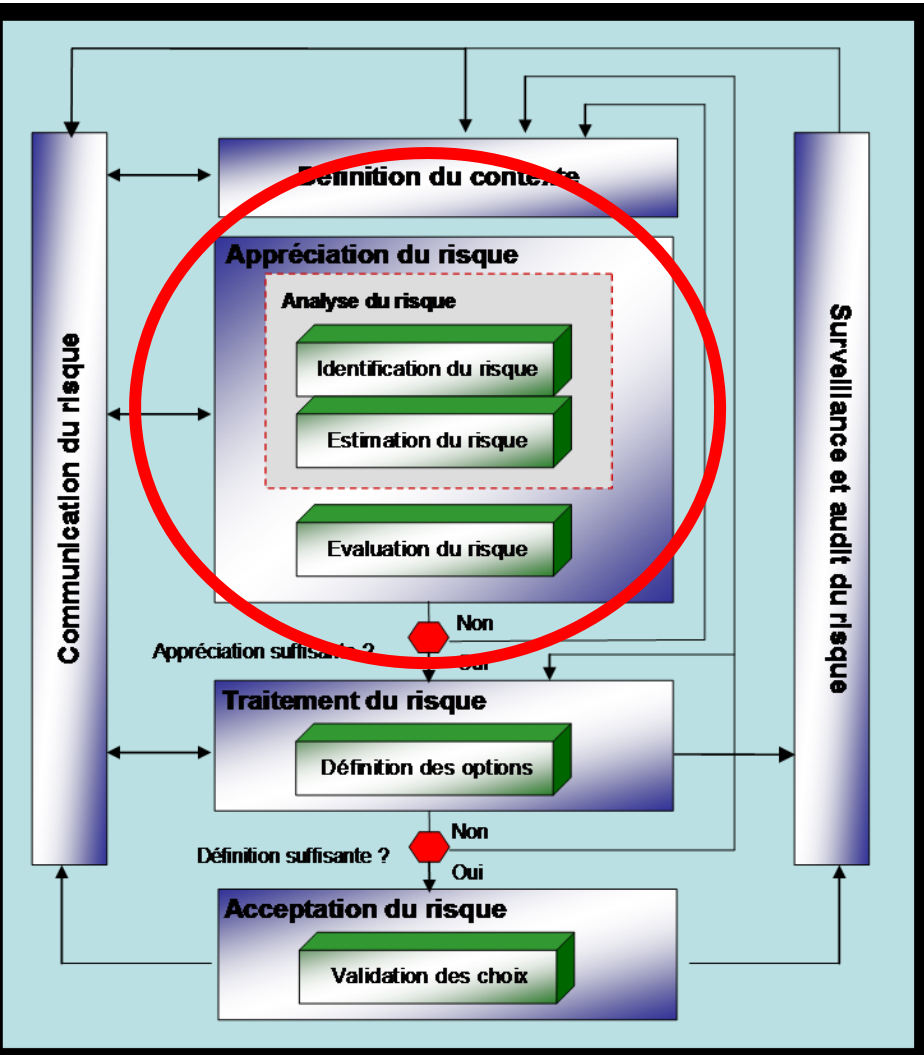
→ **Critères d'évaluation du risque**
Critères d'impact
Critères d'acceptation du risque

7.3 Définition du Domaine d'application et limites
Il convient que l'organisme définisse le domaine d'application et les limites de la gestion du risque en sécurité de l'information.

→ **Exemples : Une application**
Une infrastructure en technologie de l'information, un processus métier, une partie définie d'un organisme

7.4 Organisation de la gestion du risque en sécurité de l'information

→ **Rôles et responsabilité relatives au processus de gestion du risques**



E.1 Appréciation du risque de haut niveau en sécurité de l'information

L'appréciation de haut niveau permet de définir les priorités et la chronologie des actions. Pour différentes raisons, par exemple de budget, il peut s'avérer impossible de mettre en œuvre toutes les mesures de sécurité en même temps ; seuls les risques les plus critiques peuvent alors être abordés par le processus de traitement de risque. Il peut également être précoce de commencer une gestion détaillée de risque si la mise en œuvre n'est envisagée qu'après une ou deux années. Afin d'atteindre cet objectif, l'appréciation de haut niveau peut commencer par une évaluation de haut niveau des conséquences plutôt que par une analyse systématique des menaces, des vulnérabilités, des actifs et des conséquences.

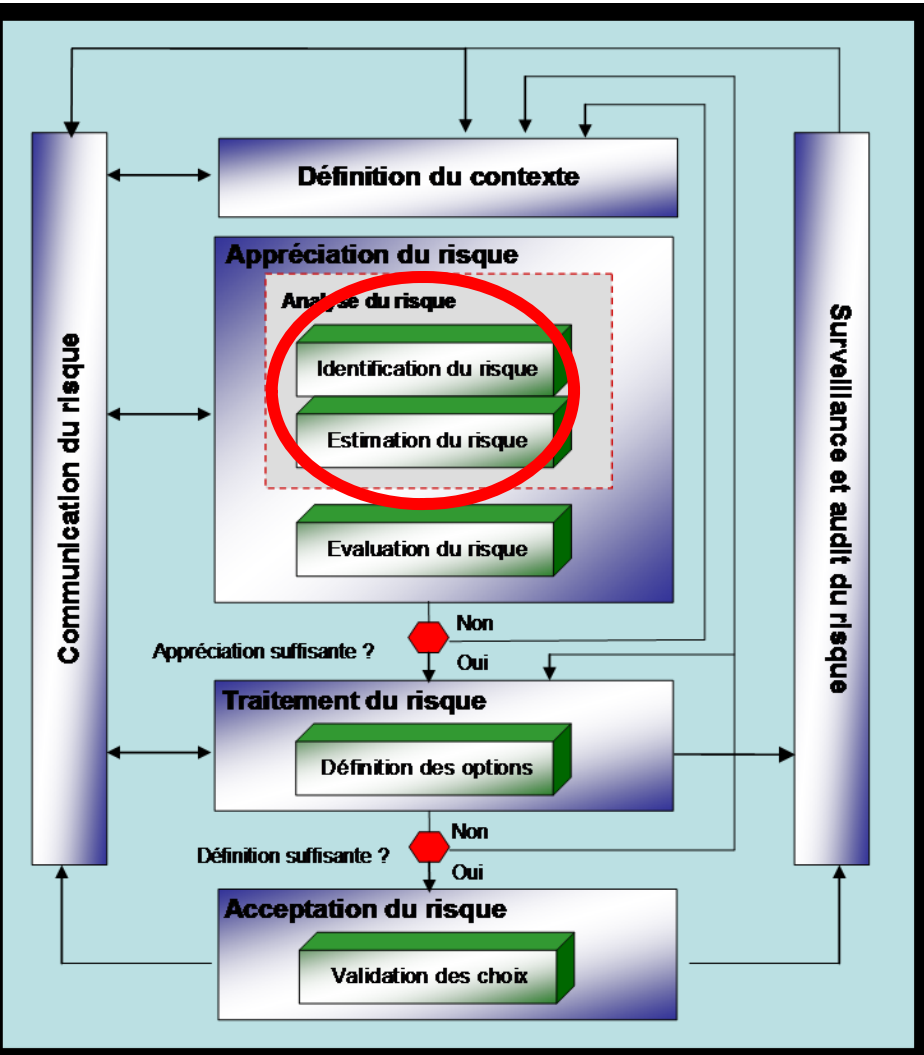
Une autre raison de commencer par l'appréciation de haut niveau est de la synchroniser avec d'autres plans relatifs à la gestion des modifications (ou la continuité de l'activité). Par exemple, il n'est pas conseillé de sécuriser entièrement un système ou une application s'il est prévu de les sous-traiter dans un futur proche, même s'il peut être encore utile de procéder à l'appréciation du risque pour définir le contrat de sous-traitance.

E.2 Appréciation détaillée du risque en sécurité de l'information

Le processus d'appréciation détaillée du risque en sécurité de l'information implique l'identification et l'évaluation approfondie des actifs, l'appréciation des menaces par rapport à ces actifs et l'appréciation des vulnérabilités. Les résultats obtenus grâce à ces activités sont alors utilisés pour apprécier les risques, puis pour identifier le traitement du risque.

Cette étape détaillée exige en général du temps, des efforts et une expertise considérables et peut, par conséquent, être la plus adaptée aux systèmes d'information présentant un risque élevé.

Norme ISO / IEC 27005



Identification du risque

Identification des actifs
Identification des menaces
Identification des vulnérabilités
Identification des conséquences
Evaluation des contrôles existants

Estimation du risque

Définition de la méthodologie
Estimation des conséquences
Estimation de l'occurrence des menaces
Evaluation des vulnérabilités
Estimation du niveau de risque

8.2.1.2 Identification des actifs

<u>Éléments d'entrée</u> : Domaine d'application et limites de l'appréciation du risque à effectuer, liste des composants avec les propriétaires, emplacement, fonction etc.

<u>Action</u> : Il convient d'identifier les actifs relevant du domaine d'application établi (conformément à l'ISO/CEI 27001, paragraphe 4.2.1 d)1)).

<u>Éléments de sortie</u> : Liste des actifs dont les risques sont à gérer et liste des processus métier relatifs aux actifs et leur pertinence.

B.1 Exemples d'identification des actifs

Afin de procéder à l'évaluation des actifs, il est nécessaire pour un organisme d'identifier ses actifs (à un niveau de détail approprié). Il est possible de distinguer deux types d'actifs :

- les actifs primordiaux :
  - processus et activités métier
  - informations
- les actifs en support (sur lesquels reposent les actifs primordiaux du domaine d'application) de tous les types :
  - matériel
  - logiciels
  - réseau
  - personnel
  - site
  - structure de l'organisme

Il existe deux types d'actifs primordiaux :

<u>1 – Les processus (ou sous processus) et activités métier, par exemple</u> :

- les processus dont la perte ou la dégradation rend impossible la réalisation de la mission de l'organisme,
- les processus contenant des processus secrets ou les processus impliquant une technique brevetée,
- les processus qui, s'ils sont modifiés, peuvent considérablement affecter l'accomplissement de la mission de l'organisme,
- les processus qui sont nécessaires à l'organisme pour être conforme aux exigences contractuelles, légales ou réglementaires.

<u>2 – Les informations</u> :

D'une façon plus générale, les informations primordiales comprennent essentiellement :

- les informations vitales pour l'exercice de la mission ou de l'activité de l'organisme,
- les informations personnelles, telles que définies de manière spécifique par la législation nationale relative à la vie privée,
- les informations stratégiques requises pour atteindre les objectifs définis par les orientations stratégiques,
- les informations à forte valeur financière dont la collecte, le stockage, le traitement et la transmission nécessitent un long délai et/ou impliquent un coût d'acquisition élevé.

Les processus et informations, qui ne sont pas jugés sensibles, après cette activité n'auront aucune classification dans le reste de l'étude. Cela signifie que même si ces processus et informations sont compromis, l'organisme parviendra malgré tout à accomplir la mission.

Toutefois, ils exigeront souvent la mise en œuvre de mesures de sécurité afin de protéger les processus et informations jugés sensibles.

CLUSIR EST

Norme ISO

Matériel
Equipement de traitement des données (actif)
Equipement automatique de traitement de l'information comprenant les éléments nécessaires pour fonctionner de manière indépendante.
Equipement transportable
Equipement informatique portable.
Equipement fixe
Equipement informatique utilisé dans les locaux de l'organisme.
Périphériques de traitement
Equipement relié à un ordinateur via un port de communication (lien en série, lien parallèle, etc.) pour saisir, transporter ou transmettre des données.
Support de données (passif) (Il s'agit de supports destinés à stocker des données ou des fonctions)
Support électronique
Support d'information pouvant être relié à un ordinateur ou à un réseau informatique afin de stocker des données (Exemples : disquette, CD ROM, cartouche de secours, disque dur amovible, clé USB, cassette)
Supports statiques et non électriques contenant des données (Exemples : papier, diapositive, transparent, documentation, fax.).
Logiciels
Les logiciels comprennent tous les programmes contribuant au fonctionnement d'un ensemble de traitement de données.
Système d'exploitation
Logiciels de service, de maintenance ou d'administration
Logiciel caractérisé par le fait qu'il complète les services du système d'exploitation et qu'il ne situe pas directement au service des utilisateurs ou des applications.
Progiciel ou logiciel standard (Exemples : logiciel de gestion de base de données, logiciel de messagerie électronique, groupware, logiciel d'annuaire, logiciel serveur, etc.)
Applications métier
Application métier standard (Exemples : logiciel de comptabilité, logiciel de commande de machines outils, logiciel d'assistance clientèle, logiciel de gestion des compétences personnelles)
Application métier spécifique (Exemples : Gestion des factures de clients d'opérateurs téléphoniques, application de surveillance en temps réel pour le lancement de fusée.)

Réseau
Supports (Exemples : Réseau téléphonique commuté public (RTCP), Ethernet, GigabitEthernet, ADSL (Ligne d'abonné numérique asymétrique), spécifications de protocole sans fil (par exemple WiFi 802.11), Bluetooth, FireWire.)
Relais actif ou passif (Exemples : pont, routeur, concentrateur, sélecteur, central automatique.)
Interface de communication (Exemples : GPRS (service général de paquets radio), adaptateur Ethernet)
Personnel
Décideur (Exemples : direction générale, chef de projet.)
Utilisateurs
Personnel d'exploitation / de maintenance (Exemples : administrateur système, administrateur de données, back-up, centre d'assistance, opérateur de télédistribution, responsables de la sécurité.)
Développeurs
Site
Environnement extérieur (Exemples : résidence du personnel, locaux d'un autre organisme, environnement situé à l'extérieur du site (zone urbaine, zone dangereuse)
Locaux (Exemples : établissement, bâtiments)
Zone (Exemples : bureaux, zone d'accès réservé, zone sécurisée)
Services essentiels
Communication (Services et matériel de télécommunications fournis par un opérateur)
Utilitaires
Services et moyens (sources et câblage) nécessaires pour alimenter le matériel et les périphériques de technologie de l'information.
Alimentation en eau
Traitement des déchets
Services et moyens (matériel, contrôle) destinés à rafraîchir et à purifier l'air.
Organisme
Autorités (Exemples : entité responsable, siège social d'un organisme)
Structure de l'organisme (Exemples : gestion des ressources humaines, gestion des technologies de l'information, gestion des achats, gestion des entités opérationnelles, service de sécurité des bâtiments, service incendie, gestion des audits)
Organisation de projet ou de système (Exemples : nouveau projet de développement d'une application, projet de migration d'un système d'information)
Sous-traitants / Fournisseurs / Fabricants (Exemples : entreprise de gestion des locaux, entreprise de sous-traitance, cabinets de consultants.)

8.2.1.3 Identification des menaces

<u>Éléments d'entrée</u> : Informations relatives aux menaces obtenues grâce au réexamen des incidents, aux propriétaires des actifs, aux utilisateurs et à d'autres sources, y compris des catalogues de menaces externes.

<u>Action</u> : Il convient d'identifier les menaces et leurs sources (conformément à l'ISO/CEI 27001, paragraphe 4.2.1 d)2)).

<u>Élément de sortie</u> : Liste de menaces avec identification du type et de la source de la menace.

Type	Menaces	Origine
Dommage physique	Incendie	A, D, E
	Dégât des eaux	A, D, E
	Pollution	A, D, E
	Accident majeur	A, D, E
	Destruction de matériel ou de support	A, D, E
	Poussière, corrosion, congélation	A, D, E
Catastrophes naturelles	Phénomène climatique	E
	Phénomène sismique	E
	Phénomène volcanique	E
	Phénomène météorologique	E
	Inondation	E
Perte de services essentiels	Panne du système de climatisation ou d'alimentation en eau	A, D
	Perte de la source d'alimentation en électricité	A, D, E
	Panne du matériel de télécommunications	A, D
Perturbation due à des rayonnements	Rayonnements électromagnétiques	A, D, E
	Rayonnements thermiques	A, D, E
	Impulsions électromagnétiques	A, D, E
Compromission d'informations	Interception de signaux d'interférence compromettants	D
	Espionnage à distance	D
	Ecoute	D
	Vol de supports ou de documents	D
	Vol de matériel	D
	Récupération de supports recyclés ou mis au rebut	D
	Divulgation	A, D
	Données provenant de sources douteuses	A, D
	Piégeage de matériel	D
	Piégeage de logiciel	A, D
	Géolocalisation	D
Défaillances techniques	Panne de matériel	A
	Dysfonctionnement du matériel	A
	Saturation du système d'information	A, D
	Dysfonctionnement du logiciel	A
	Violation de la maintenabilité du système d'information	A, D
Actions non autorisées	Utilisation non autorisée du matériel	D
	Reproduction frauduleuse de logiciel	D
	Utilisation de logiciels copiés ou de contrefaçon	A, D
	Corruption de données	D
	Traitement illégal de données	D
Compromission des fonctions	Erreur d'utilisation	A
	Abus des droits	A, D
	Usurpation de droits	D
	Déni d'actions	D
	Violation de la disponibilité du personnel	A, D, E

Il convient de prêter une attention particulière aux sources de menace humaines. Ces sources sont présentées en détail de manière spécifique dans le tableau suivant :

Origine de la menace	Motivation	Conséquences possibles
Pirate informatique	Défi Amour-propre Rébellion Statut Argent	• Piratage informatique • Ingénierie sociale • Intrusion, introductions par effraction dans un système • Accès non autorisé dans un système
Escroc informatique	Destruction d'informations Divulgation illégale d'informations Gain financier Modification non autorisée de données	• Délit informatique (par exemple harcèlement par Internet) • Acte frauduleux (par exemple réémission, usurpation d'identité, interception) • Corruption d'informations • Usurpation • Intrusion dans un système
Terroriste	Chantage Destruction Exploitation Vengeance Avantage politique Couverture médiatique	• Bombe/Terrorisme • Guerre de l'information • Attaque du système (par exemple déni de service distribué) • Pénétration dans un système • Piégeage d'un système
Espionnage industriel (Renseignement, entreprises, gouvernements étrangers, intérêts d'autres gouvernements)	Avantage concurrentiel Espionnage économique	• Avantage en matière de défense • Avantage politique • Exploitation économique • Vol d'informations • Intrusion dans la vie privée • Ingénierie sociale • Pénétration dans un système • Accès non autorisé à un système (accès à des informations classées, propriétaires et/ou liées à la technologie)
Initiés (employés peu qualifiés, mécontents, malveillants, négligents, malhonnêtes ou ex-employés)	Curiosité Amour-propre Renseignement Gain financier Vengeance Erreurs et omissions involontaires (par exemple erreur de saisie des données, erreur de programmation)	• Agression d'un employé • Chantage • Exploration d'informations propriétaires • Malveillance informatique • Fraude et vol • Corruption d'informations • Saisie de données falsifiées, corrompues • Interception • Code malveillant (par exemple virus, bombe logique, cheval de Troie) • Vente d'informations personnelles • Bugs du système • Intrusion dans un système • Sabotage d'un système • Accès non autorisé dans un système

8.2.1.4 Identification des mesures de sécurité existantes

Éléments d'entrée : Documentation relative aux mesures de sécurité, plans de mise en œuvre du traitement du risque.

Action : Il convient d'identifier les mesures de sécurité existantes et prévues.

Éléments de sortie : Liste de toutes les mesures de sécurité existantes et prévues, l'état relatif à leur mise en œuvre et à leur utilisation.

8.2.1.5 Identification des vulnérabilités

Éléments d'entrée : Liste des menaces connues, listes des actifs et des mesures de contrôle existantes.

Action : Il convient d'identifier les vulnérabilités susceptibles d'être exploitées par des menaces pour nuire aux actifs ou à l'organisme (conformément à l'ISO/CEI 27001, paragraphe 4.2.1 d)3)).

Éléments de sortie : Liste des vulnérabilités liées aux actifs, aux menaces et aux mesures de sécurité ; liste des vulnérabilités qui ne sont pas liées à une menace identifiée pour réexamen

Types	Exemples de vulnérabilités	
Matériel	Maintenance insuffisante/mauvaise installation des supports de stockage	V d
	Absence de programmes de remplacement périodique	D
	Sensibilité à l'humidité, à la poussière, aux salissures	P
	Sensibilité aux rayonnements électromagnétiques	R
	Absence de contrôle efficace de modification de configuration	E
	Sensibilité aux variations de tension	P é
	Sensibilité aux variations de température	P
	Stockage non protégé	V
	Manque de prudence lors de la mise au rebut	V
	Reproduction non contrôlée	V
Logiciel	Tests de logiciel absents ou insuffisants	A
	Failles bien connues dans le logiciel	A
	Pas de fermeture de session en quittant le poste de travail	A
	Mise au rebut et réutilisation de supports de stockage sans véritable effacement	A
	Absence de traces d'audit	A
	Attribution erronée des droits d'accès	A
	Logiciel distribué à grande échelle	D
	Application de programmes de gestion à de mauvaises données en termes de temps	D
	Interface utilisateur compliquée	E
	Absence de documentation	E
	Réglage incorrect de paramètres	E
	Dates incorrectes	E

Types	Exemples de vulnérabilités	
Logiciel (fin)	Absence de mécanismes d'identification et d'authentification tels que l'authentification des utilisateurs	U
	Tableaux de mots de passe non protégés	U
	Mauvaise gestion des mots de passe	U
	Activation de services non nécessaires	T
	Logiciel neuf ou en phase de rodage	D
	Spécifications des développeurs confuses ou incomplètes	D
	Absence de contrôle efficace des modifications	D
	Chargement et utilisation non contrôlés du logiciel	P
	Absence de copies de sauvegarde	P
	Absence de protection physique du bâtiment, des portes et des fenêtres	V
	Impossibilité de produire les comptes-rendus de gestion	U
Réseau	Absence de preuves d'envoi ou de réception d'un message	D
	Voies de communication non protégées	E
	Trafic sensible non protégé	E
	Mauvais câblage	P
	Point de défaillance unique	P
	Absence d'identification et d'authentification de l'expéditeur et du destinataire	U
	Architecture réseau non sécurisée	E
	Transfert de mots de passe en clair	E
	Gestion réseau inadaptée (résilience du routage)	S
	Connexions au réseau public non protégées	U
Personnel	Absence de personnel	V
	Procédures de recrutement inadaptées	D
	Formation insuffisante à la sécurité	E
	Utilisation incorrecte du logiciel et du matériel	E
	Absence de sensibilisation à la sécurité	E
	Absence de mécanismes de surveillance	T
	Travail non surveillé d'une équipe extérieure ou de l'équipe d'entretien	V
	Absence de politiques relatives à la bonne utilisation de supports de télécommunications et de la messagerie	U

Types	Exemples de vulnérabilités	
Site	Utilisation inadaptée ou négligente du contrôle d'accès physique aux bâtiments et aux salles	De
	Emplacement situé dans une zone sujette aux inondations	In
	Réseau électrique instable	Pe él
	Absence de protection physique du bâtiment, des portes et des fenêtres	Vo
Organisme	Absence de procédure formelle relative à l'enregistrement et au retrait des utilisateurs	Ab
	Absence de processus formel relatif au réexamen des droits d'accès (supervision)	Ab
	Absence de dispositions suffisantes (relatives à la sécurité) dans les contrats avec des clients et/ou des tiers	Ab
	Absence de procédure de surveillance des moyens de traitement de l'information	Ab
	Absence d'audits réguliers (supervision)	Ab
	Absence de procédures d'identification et d'appréciation du risque	Ab
	Absence de rapports d'erreur enregistrés dans les journaux administrateurs et les journaux opérations	Ab
	Réponse inadaptée du service de maintenance	Vio d'i
	Accord de service absent ou insuffisant	Vio d'i
	Absence de procédure de contrôle des modifications	Vio d'i
	Absence de procédure formelle du contrôle de la documentation SMSI	Co
	Absence de procédure formelle de supervision des enregistrements SMSI	Co
	Absence de processus formel d'autorisation des informations à disposition du public	Do
	Absence de bonne attribution des responsabilités en sécurité de l'information	Dé
	Absence de plans de continuité	Pa
	Absence de politique relative à l'utilisation des emails	En
	Absence de procédures d'introduction d'un logiciel dans des systèmes d'exploitation	En

Types	Exemples de vulnérabilités
Organisme (fin)	Absence d'enregistrements dans les journaux administrateurs et journaux opérations
	Absence de procédures relatives au traitement de l'information classée
	Absence de responsabilités en sécurité de l'information dans les descriptions de poste
	Dispositions absentes ou insuffisantes (relatives à la sécurité de l'information) dans les contrats avec les employés
	Absence de processus disciplinaire défini en cas d'incident en sécurité de l'information
	Absence de politique formelle relative à l'utilisation des ordinateurs portables
	Absence de contrôle des actifs situés hors des locaux
	Politique absente ou insuffisante relative au « bureau propre et à l'écran vide »
	Absence d'autorisation relative aux moyens de traitement de l'information
	Absence de mécanismes de surveillance établis pour des violations de sécurité
	Absence de revues de direction régulières
	Absence de procédures de signalement des failles de sécurité
	Absence de procédures de la conformité des dispositions aux droits de propriété intellectuelle

8.2.1.6 Identification des conséquences

<u>Éléments d'entrée</u> : Liste des actifs, liste des processus métier et liste des menaces et vulnérabilités, le cas échéant, liées aux actifs et leur pertinence.

<u>Action</u> : Il convient d'identifier les conséquences que des pertes de confidentialité, d'intégrité et de disponibilité peuvent avoir sur les actifs (voir l'ISO/CEI 27001 4.2.1 d) 4)).

<u>Élément de sortie</u> : Liste des scénarii d'incident et de leurs conséquences liées aux actifs et aux processus métier.

Il convient que les organismes identifient les conséquences opérationnelles des scénarii d'incident en termes de (sans s'y limiter) :

- **temps d'investigation et de réparation,**
- **temps (de travail) perdu,**
- **perte d'opportunités,**
- **santé et sûreté,**
- **coût financier des compétences spécifiques nécessaires pour réparer les dommages,**
- **image et valorisation financière de l'entreprise.**

8.2.2 Estimation du risque

8.2.2.1 Méthodologies d'estimation du risque

L'analyse de risque peut être effectuée à différents niveaux de détail selon la criticité des actifs, la portée des vulnérabilités connues et des incidents antérieurs expérimentés au sein de l'organisme.
Selon les circonstances, une méthodologie d'estimation peut être qualitative, quantitative ou une combinaison des deux.

En pratique, l'estimation qualitative est souvent utilisée en premier lieu pour obtenir une indication générale du niveau de risque et pour mettre en exergue les principaux risques. Il peut ensuite être nécessaire d'entreprendre une analyse plus spécifique ou quantitative des risques majeurs, étant donné qu'il est souvent moins complexe et moins onéreux d'effectuer une analyse qualitative qu'une analyse quantitative.

Il convient que le type d'analyse menée soit cohérent avec les critères d'évaluation du risque définis lors de l'établissement du contexte.

8.2.2.2 Appréciation des conséquences

Élément d'entrée : Liste de scénarii d'incident pertinents identifiés, incluant l'identification des menaces, vulnérabilités, actifs altérés, conséquences pour les actifs et les processus métier.

Action : Il convient d'apprécier l'impact sur l'activité de l'organisme pouvant résulter d'incidents de sécurité de l'information potentiels ou avérés, en tenant compte des conséquences d'une atteinte à la sécurité de l'information telle qu'une perte de confidentialité, d'intégrité ou de disponibilité des actifs (conformément à l'ISO/CEI 27001, paragraphe 4.2.1 e) 1)).

Élément de sortie : Liste des conséquences d'un scénario d'incident appréciées et exprimées en cohérence avec les actifs et les critères d'impact.

8.2.2.3 Appréciation de la vraisemblance d'un incident

Éléments d'entrée : Liste des scénarii d'incident pertinents identifiés, incluant l'identification des menaces, actifs affectés, vulnérabilités exploitées et conséquences pour les actifs et les processus métier. De plus, la liste de toutes les mesures de sécurité existantes et prévues, leur efficacité et l'état relatif à leur mise en œuvre et à leur utilisation.

Action : Il convient d'apprécier la vraisemblance des scénarii d'incident (conformément à l'ISO/CEI 27001, paragraphe 4.2.1 e)2)).

Élément de sortie : Vraisemblance des scénarii d'incident (quantitative ou qualitative).

8.2.2.4 Estimation du niveau de risque

<u>Élément d'entrée</u> : Liste des scénarii d'incident accompagnés de leurs conséquences liées aux actifs et aux processus métier, ainsi que leur vraisemblance (quantitative ou qualitative).

<u>Action</u> : Il convient d'estimer le niveau de risque de tous les scénarii d'incident pertinents (conformément à l'ISO/CEI 27001, paragraphe 4.2.1 e)4)).

<u>Élément de sortie</u> : Liste des risques avec un niveau de risque valorisé

E.2.1 Exemple 1 Matrice avec valeurs prédéfinies

Dans les méthodes d'appréciation du risque de ce type, les actifs physiques réels ou proposés sont évalués en termes de coût de remplacement ou de reconstruction (c'est-à-dire des mesures quantitatives). Ces coûts sont ensuite convertis sur une échelle qualitative identique à celle utilisée pour les informations (voir ci-dessous)

Tableau E.1a)

	Vraisemblance – Menace	Faible			Moyenne			Élevée		
	Facilité d'exploitation	F	M	E	F	M	E	F	M	E
Valeur de l'actif	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Tableau E.1b)

	Vraisemblance d'un scénario d'incident	Très faible (Très peu probable)	Faible (Peu probable)	Moyenne (Possible)	Élevée (Probable)	Très élevée (Fréquente)
Impact sur l'activité	Très faible	0	1	2	3	4
	Faible	1	2	3	4	5
	Moyen	2	3	4	5	6
	Élevé	3	4	5	6	7
	Très élevé	4	5	6	7	8

E.2.2 Exemple 2 – Classement des menaces par mesures de risque

Une matrice, ou un tableau identique au tableau E.2, peut être utilisée pour relier les facteurs des conséquences (valeur des actifs) et la vraisemblance des menaces (en tenant compte des aspects des vulnérabilités). La première étape consiste à évaluer les conséquences (valeur de l'actif) de chaque actif menacé sur une échelle prédéfinie, allant par exemple de 1 à 5 (colonne « b » dans le tableau). La seconde étape consiste à évaluer la vraisemblance de chaque menace sur une échelle prédéfinie, allant par exemple de 1 à 5 (colonne « c » dans le tableau). La troisième étape consiste à calculer la mesure du risque en multipliant (b x c). Les menaces peuvent finalement être classées selon l'ordre de leur mesure de risque associée. Noter que dans cet exemple, 1 est considéré comme la conséquence et la vraisemblance la plus faible.

Tableau E.2

Descripteur de menace (a)	Valeur de la conséquence (actif) (b)	Vraisemblance de la menace (c)	Mesure du risque (d)	Classement des menaces (e)
Menace A	5	2	10	2
Menace B	2	4	8	3
Menace C	3	5	15	1
Menace D	1	3	3	5
Menace E	4	1	4	4
Menace F	2	4	8	3

E.2.3 Exemple 3 – Appréciation d'une valeur relative à la vraisemblance et aux conséquences possibles des risques

Dans cet exemple, l'accent est mis sur les conséquences des incidents en sécurité de l'information (c'est-à-dire les scénarii d'incident), et sur la détermination des systèmes qu'il convient de considérer comme prioritaires. Cette appréciation s'effectue en appréciant deux valeurs pour chaque actif et risque, ce qui permet de déterminer la note correspondant à chaque actif. Lors de l'ajout de l'ensemble des notes des actifs du système, la mesure de risque de ce système est déterminée.

Une valeur est d'abord attribuée à chaque actif. Cette valeur correspond aux conséquences défavorables éventuelles susceptibles d'apparaître si l'actif est menacé. Pour chaque menace applicable à l'actif, cette valeur est attribuée à l'actif.

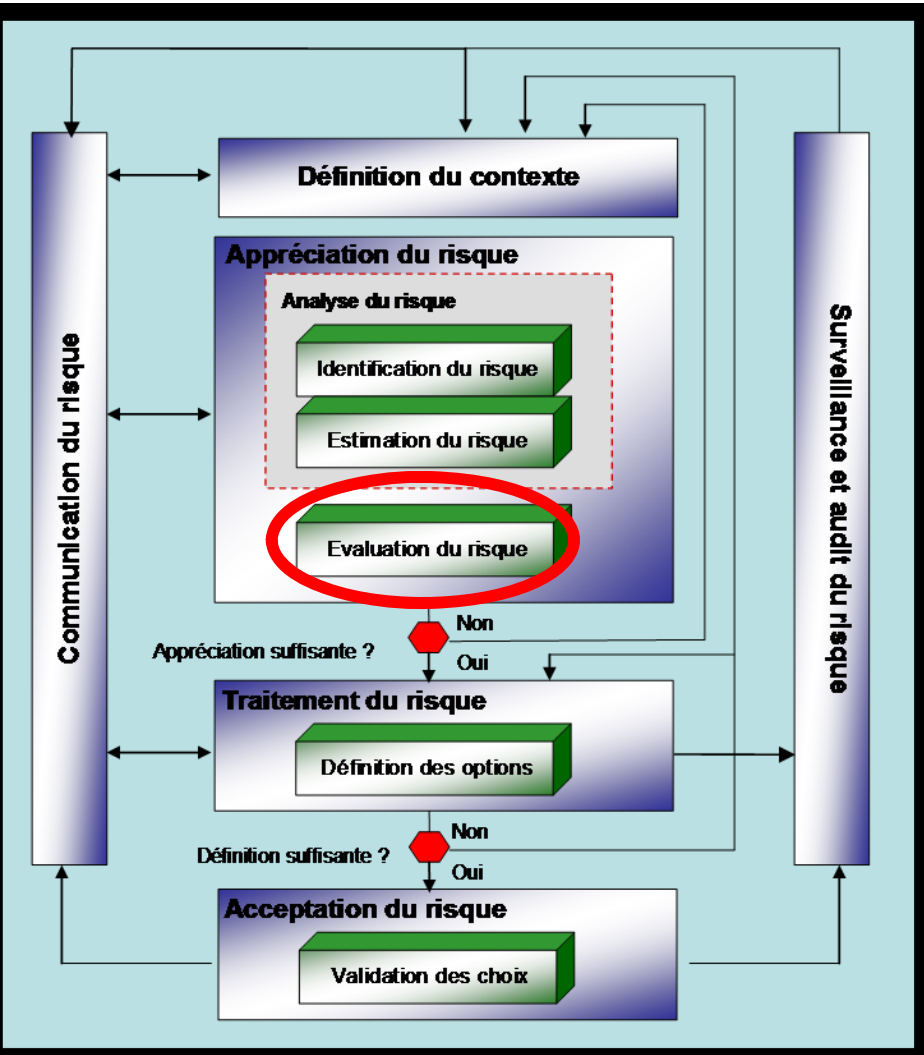
Une valeur de vraisemblance est ensuite appréciée. Elle est appréciée en combinant la vraisemblance de la menace et la facilité d'exploitation de la vulnérabilité, voir le Tableau E.3 exprimant la vraisemblance d'un scénario d'incident.

Tableau E.3

Vraisemblance de la menace	Faible			Moyenne			Élevée		
Niveaux de vulnérabilité	F	M	E	F	M	E	F	M	E
Valeur de la vraisemblance d'un scénario d'incident	0	1	2	1	2	3	2	3	4

Tableau 4

Valeur de l'actif	0	1	2	3	4
Valeur de la vraisemblance					
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8



8.3 Evaluation du risque

Éléments d'entrée : Liste des risques avec un niveau de risque valorisé et critères d'évaluation du risque.

Action : Il convient de comparer le niveau des risques aux critères d'évaluation du risque et aux critères d'acceptation du risque (conformément à l'ISO/CEI 27001, paragraphe 4.2.1 e) 4)).

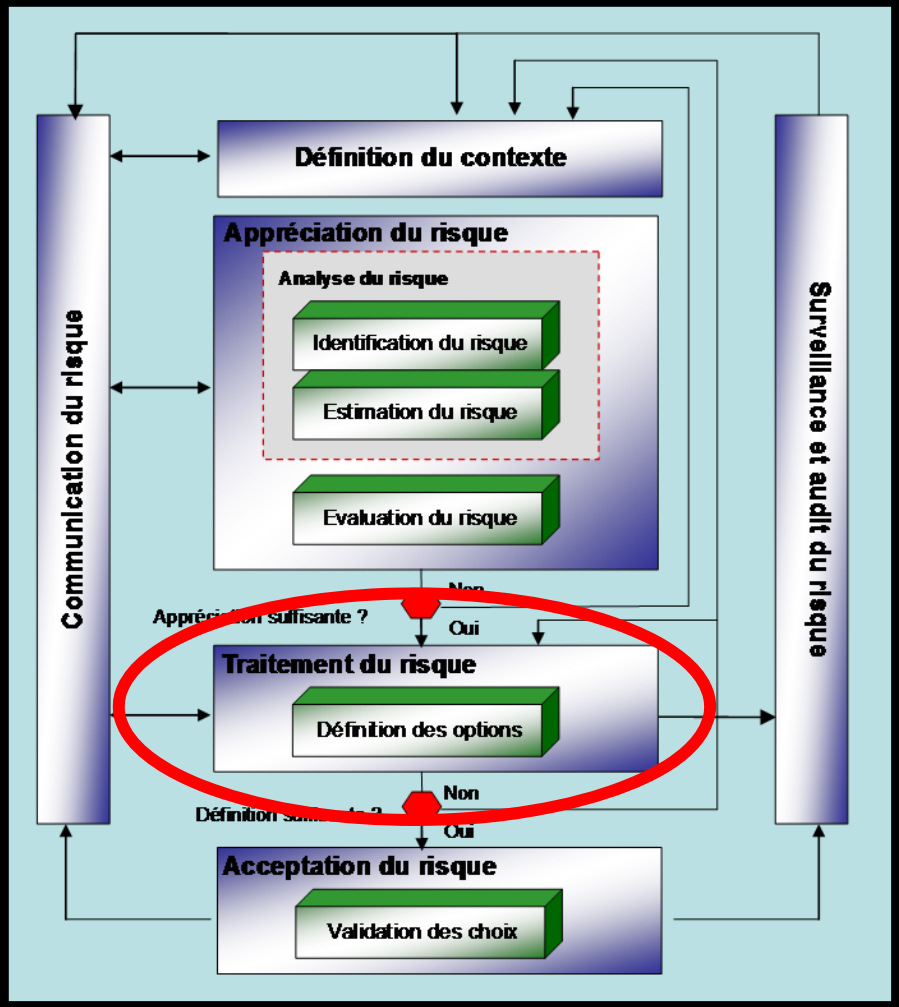
Élément de sortie : Liste des risques classés par ordre de priorité selon les critères d'évaluation du risque en relation avec les scénarii d'incident qui conduisent à ces risques

Critères d'évaluation du risque

Il convient d'élaborer des critères d'évaluation du risque afin d'évaluer le risque de l'organisme en sécurité de l'information en prenant en compte les éléments suivants :

- la valeur stratégique des processus informationnels métier,
- la criticité des actifs informationnels concernés,
- les exigences légales et réglementaires ainsi que les obligations contractuelles,
- l'importance opérationnelle et métier de la disponibilité, de la confidentialité et de l'intégrité,
- les attentes et les perceptions des parties prenantes ainsi que les conséquences négatives sur la valorisation financière et la réputation de l'organisme.

En outre, les critères d'évaluation du risque peuvent être utilisés pour spécifier les priorités du traitement du risque.

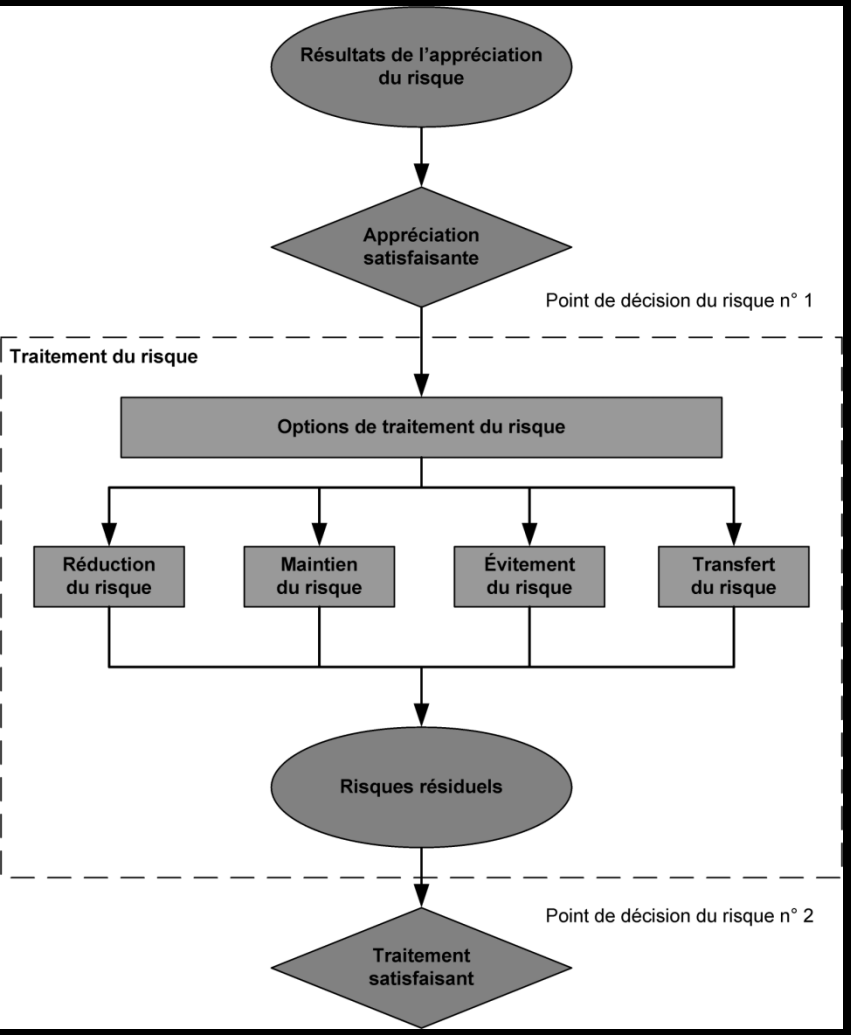


9.1 Description générale du traitement du risque

<u>Élément d'entrée</u> : Liste des risques classés par ordre de priorité en cohérence avec les critères d'évaluation du risque et en relation avec les scénarii d'incident qui conduisent à ces risques.

<u>Action</u> : Il convient de choisir des mesures de sécurité pour réduire, maintenir, éviter ou transférer les risques, et de définir un plan de traitement du risque.

<u>Éléments de sortie</u> : Plan de traitement du risque et risques résiduels soumis à la décision d'acceptation des dirigeants de l'organisme



9.2 Réduction du risque

Action : Il convient de réduire le niveau de risque par la sélection des mesures de sécurité afin que le risque résiduel puisse être réapprécié et jugé acceptable

9.3 Maintien du risque

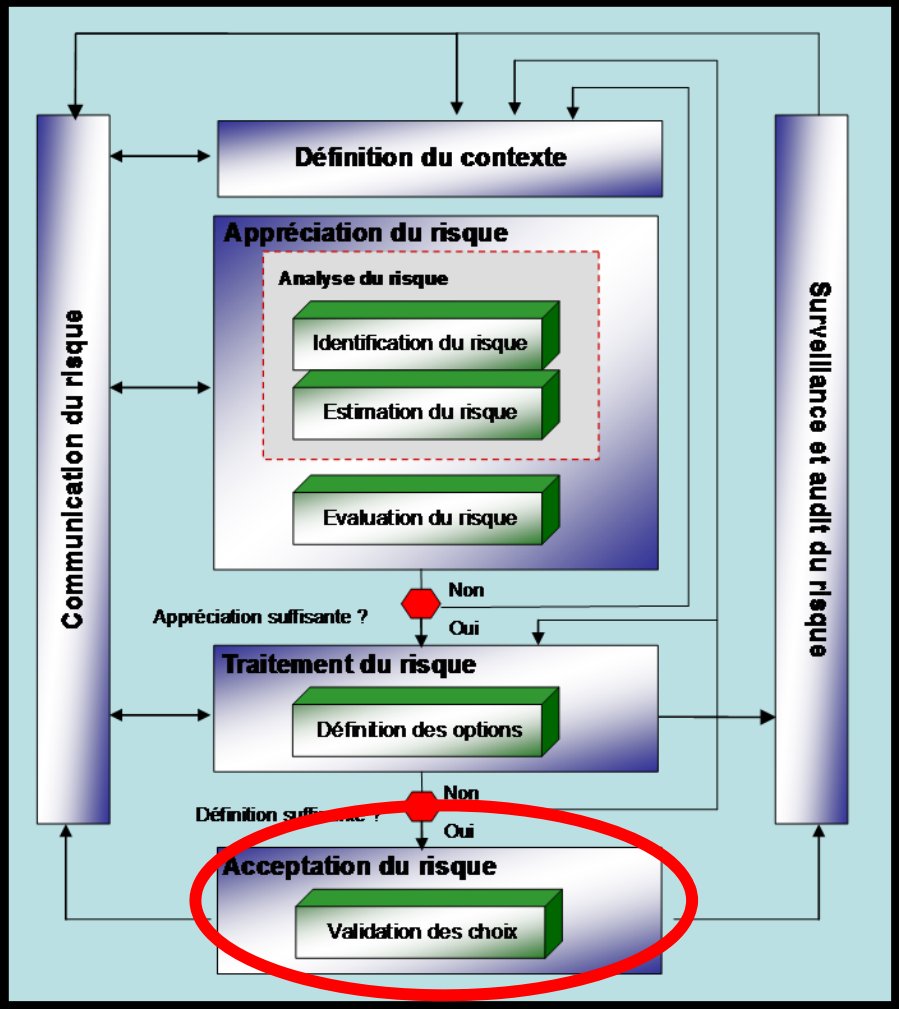
Action : Il convient de prendre la décision de maintenir le risque sans autre action en fonction de l'évaluation du risque.

9.4 Évitement du risque

Action : Il convient d'éviter l'activité ou la situation qui donne lieu à un risque particulier.

9.5 Transfert du risque

Action : Il convient de transférer le risque à une autre partie capable de gérer de manière plus efficace le risque spécifique en fonction de l'évaluation du risque



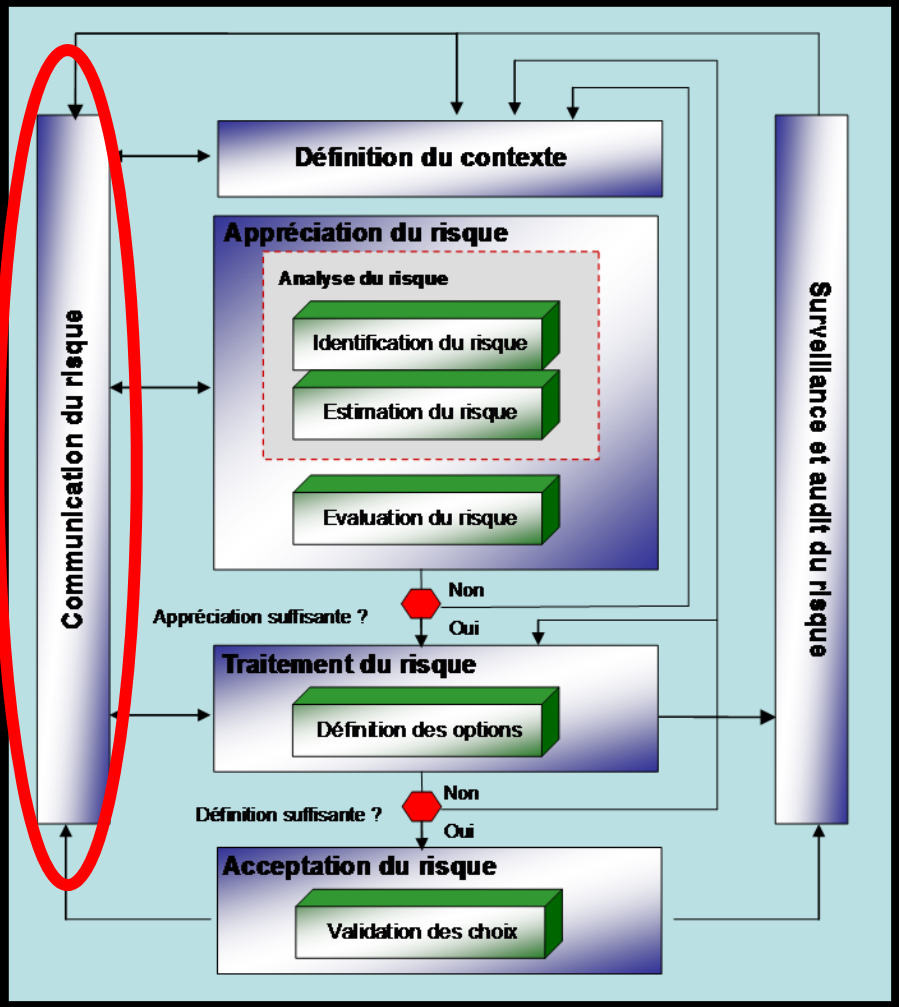
La Direction Générale doit valider le plan de traitement des risques.
Elle peut accepter des risques en toute connaissance de cause.
Les décisions doivent être formalisées

10 Acceptation du risque en sécurité de l'information

<u>Éléments d'entrée</u> : Plan de traitement du risque et appréciation du risque résiduel soumis à la décision d'acceptation des dirigeants de l'organisme.

<u>Action</u> : Il convient de prendre la décision d'accepter les risques et les responsabilités de cette décision et de l'enregistrer formellement (conformément à l'ISO/CEI 27001 paragraphe 4.2.1 h)).

<u>Élément de sortie</u> : Liste des risques acceptés et justification pour les risques ne remplissant pas les critères normaux d'acceptation du risque de l'organisme



Il convient qu'un organisme élabore des plans de communication du risque en fonctionnement normal ainsi que dans les situations d'urgence.

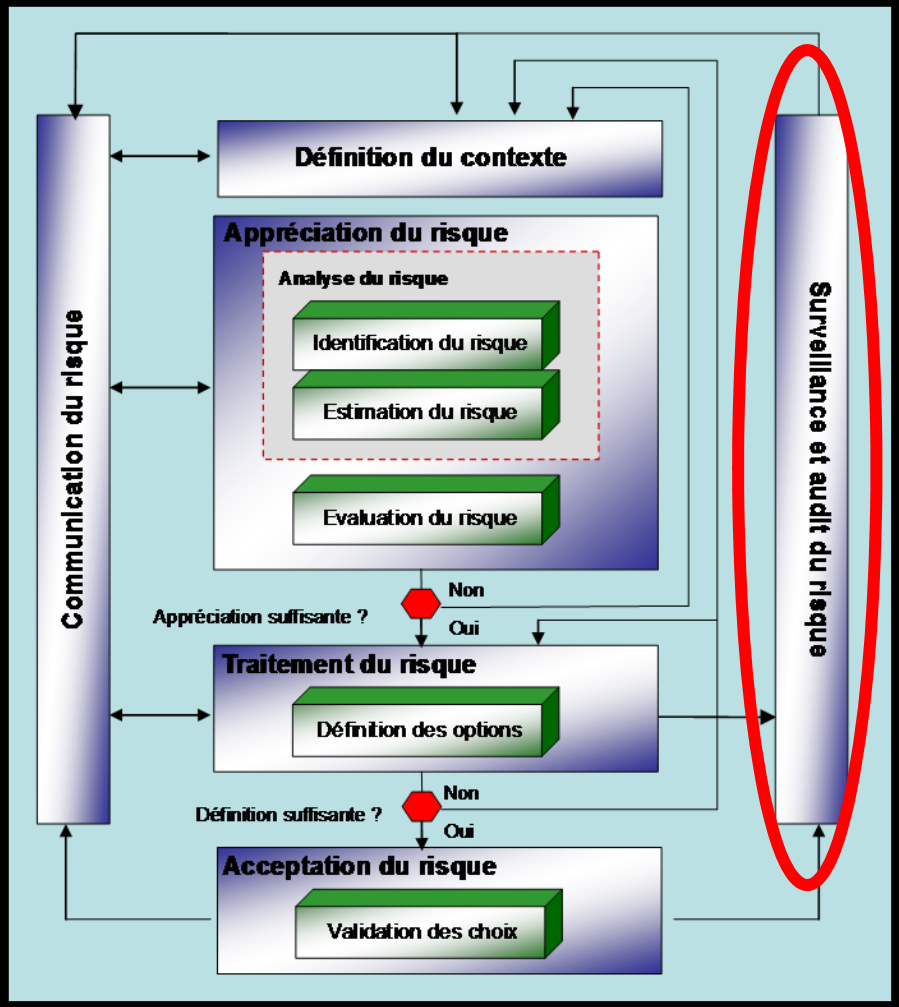
Par conséquent, il convient de procéder de manière continue à l'activité de communication du risque

11 Communication du risque en sécurité de l'information

<u>Éléments d'entrée</u> : L'ensemble des informations, relatives au risque, obtenues grâce aux activités de gestion du risque (voir la Figure 1).

<u>Action</u> : Il convient d'échanger et/ou de partager les informations relatives au risque entre le décideur et les autres parties prenantes.

<u>Élément de sortie</u> : Compréhension permanente du processus et des résultats de la gestion du risque en sécurité de l'information de l'organisme



Les risques ne sont pas statiques. Les menaces, les vulnérabilités, la vraisemblance ou les conséquences peuvent changer brutalement sans aucune indication préalable.

Par conséquent, une surveillance constante est nécessaire pour détecter ces changements.

Cette surveillance peut être assurée par des services externes qui fournissent des informations relatives à de nouvelles menaces ou vulnérabilités

12.1 Surveillance et réexamen des facteurs de risque

Élément d'entrée : L'ensemble des informations, relatives au risque, obtenues grâce aux activités de gestion du risque.

Action : Il convient de surveiller et de réexaminer les risques et leurs facteurs (à savoir valeur des actifs, impacts, menaces, vulnérabilités et vraisemblance) pour identifier au plus tôt toutes les modifications dans le contexte de l'organisme et pour maintenir une cartographie complète des risques.

Éléments de sortie : Alignement continu de la gestion du risque avec les objectifs métiers de l'organisme ainsi qu'avec les critères d'acceptation du risque.

12.2 Surveillance, réexamen et amélioration de la gestion du risque

Éléments d'entrée : L'ensemble des informations, relatives au risque, obtenues grâce aux activités de gestion du risque (voir la Figure 1).

Action : Il convient de constamment surveiller, réexaminer et améliorer le processus de gestion du risque en sécurité de l'information si nécessaire et de manière appropriée

Élément de sortie : Pertinence permanente du processus de gestion du risque en sécurité de l'information avec les objectifs métiers de l'organisme ou mise à jour du processus.

CONCLUSION

La norme ISO 27005 va probablement devenir incontournable.

Elle sera utilisée dans le cadre de la mise en œuvre d'un ISMS et dans la mise en œuvre d'un processus de gestion des risques.

Les méthodes Françaises (Méhari et Ebios) vont évoluer vers une conformité à l'ISO 27005.

Merci de votre attention