Annexe 2 - Tables des exemples type

Contenu

Exemple d'action type 1.1.1. Cadrer l'étude des risques

Exemple

L'objectif de l'étude : gérer les risques SSI sur le long terme et élaborer une politique

Le directeur de la société @RCHIMED souhaite que les risques de sécurité de l'information qui pourraient empêcher l'organisme d'atteindre ses objectifs soient gérés, et ce, de manière continue, afin d'être au plus proche d'une réalité en mouvement.

Une politique de sécurité de l'information doit ainsi être produite, appliquée et contrôlée.

Par ailleurs, il n'exclut pas l'idée de faire certifier à terme les principales activités du cabinet selon l'ISO 27001 et reconnaît l'intérêt d'exploiter des meilleures pratiques reconnues internationalement (ISO 27002). Par conséquent, une déclaration d'applicabilité devrait être produite ultérieurement.

Le plan d'action : une réflexion sur 15 jours qui requiert la participation de tous

Pour ce faire, le cabinet @RCHIMED prévoit la structure de travail suivante :

Activités d'EBIOS	***Directeur***	***Directeur adjoint***	***Comité de suivi***	***Secrétariat***	***Service commercial***	***Bureau d'études***	***Service comptabilité***	***Documents à produire en plus de l'étude des risques***	***Consignes particulières***	***Ressources estimées (en h.j)***	***Durée (en jours)***
Activité 1.1 - Définir le cadre de la gestion des risques		*R*	*C*	*I*	*I*	*I*	*I*			*2*	*2*
Activité 1.2 - Préparer les métriques		*R*	*C*	*I*	*I*	*I*	*I*		*Vérifier l'uniformité de la compréhension*	*2*	*2*
Activité 1.3 - Identifier les biens	*A*	*R*	*C*	*C*	*C*	*C*	*I*	*Note de cadrage*	*Ne pas trop détailler*	*6*	*2*
Activité 2.1 - Apprécier les événements redoutés		*R*	*C*	*C*	*C*	*C*	*I*		*Utiliser les bases génériques*	*6*	*2*
Activité 3.1 - Apprécier les scénarios de menaces		*R*	*C*	*C*	*C*	*C*	*I*		*Utiliser les bases génériques*	*6*	*2*
Activité 4.1 - Apprécier les risques		*R*	*C*	*I*	*I*	*I*	*I*			*1*	*1*
Activité 4.2 - Identifier les objectifs de sécurité	*A*	*R*	*C*	*I*	*I*	*I*	*I*	*Note de stratégie*		*2*	*1*
Activité 5.1 - Formaliser les mesures de sécurité à mettre en œuvre	*A*	*R*	*C*	*C*	*C*	*C*	*I*	*Politique de sécurité de l'information*		*15*	*3*
Activité 5.2 - Mettre en œuvre les mesures de sécurité	*A*	*R*	*I*	*C*	*C*	*C*	*I*	*Homologation*	*Cette activité ne sera réalisée de suite*	*0*	*0*

Légende : R = Réalisation ; A = Approbation ; C = Consultation ; I = Information

Exemple d'action type 1.1.2. Décrire le contexte général

Exemple

L'organisme étudié est la société @RCHIMED. Il s'agit d'une PME toulonnaise constituée d'une douzaine de personnes. C'est un bureau d'ingénierie en architecture qui réalise des plans d'usines et d'immeubles. Sa vocation principale est de vendre des services pour les professionnels du bâtiment.

@RCHIMED compte de nombreux clients, privés ou publics, ainsi que quelques professionnels du bâtiment.

Son capital s'élève à xxxxx € et son chiffre d'affaires à yyyyy €.

Ses missions consistent principalement à élaborer des projets architecturaux, ainsi que des calculs de structures et la création de plans techniques.

Ses valeurs sont la réactivité, la précision des travaux, la créativité architecturale et la communication. Les principaux métiers représentés sont l'architecture et l'ingénierie du bâtiment.

Sa structure organisationnelle est fonctionnelle avec une direction, un service commercial, un bureau d'études, un service comptabilité et un service de gestion de site internet.

Ses axes stratégiques sont d'une part l'utilisation des nouvelles technologies (Internet, Intranet) dans un but d'ouverture vers l'extérieur et d'optimisation des moyens, et d'autre part la consolidation de l'image de marque (protection des projets sensibles).

Ses principaux processus métiers sont les suivants :

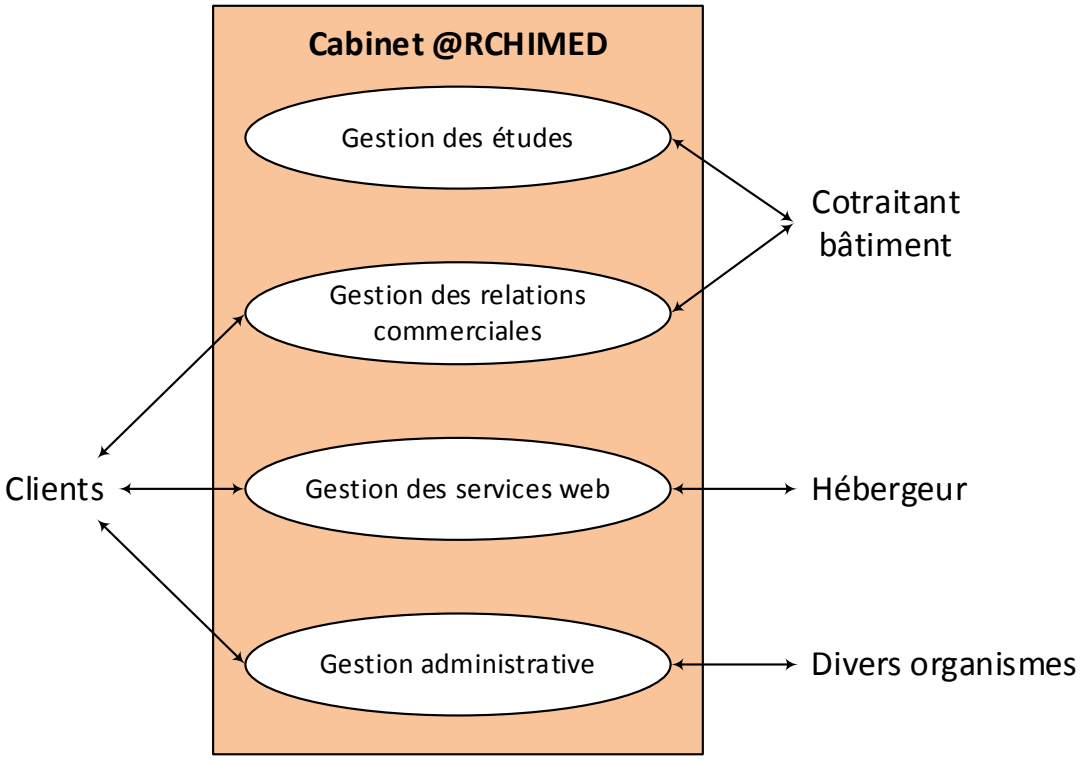


Figure 1 - ***Les principaux processus métiers de la société***

Plusieurs éléments de conjoncture ont été identifiés :

- la mise en réseau des systèmes informatiques s'est effectuée avec succès et a permis de réduire encore plus les délais de réalisation des travaux ;
- l'entreprise a dernièrement perdu un marché : la rénovation de la mairie de Draguignan. Lors de la présentation des projets, il est apparu de curieuses similitudes entre la maquette virtuelle d'@RCHIMED et la proposition d'un concurrent de Nice. Le directeur d'@RCHIMED soupçonne une compromission du projet qu'il avait présenté. Il a maintenant des craintes sur la confidentialité de certains projets ;
- l'arsenal de Toulon semble vouloir rénover certaines installations servant à la maintenance des bâtiments de la marine nationale. @RCHIMED souhaiterait pouvoir se présenter à d'éventuels appels d'offres ;
- une rude concurrence, dépendant des appels d'offres, s'exerce dans le secteur ;
- seule une crise très grave dans le bâtiment pourrait affecter le fonctionnement du cabinet d'architecture.

Une gestion des risques intégrée

Le risque est défini comme un "scénario, avec un niveau donné, combinant un événement redouté par @RCHIMED sur son activité, et un ou plusieurs scénarios de menaces. Son niveau correspond à l'estimation de sa vraisemblance et de sa gravité".

En matière de gestion des risques, les rôles et responsabilités sont les suivants :

- le directeur d'@RCHIMED est pleinement responsable des risques pesant sur sa société ;
- le directeur adjoint a été mandaté pour animer la gestion des risques de sécurité de l'information ; il est ainsi responsable de la réalisation des études de risques ;
- un comité de suivi, composé d'un membre de chaque service et présidé par le directeur adjoint, réalisera la première étude de risques et se réunira ensuite tous les six mois afin de faire le point sur les évolutions à apporter à la gestion des risques de sécurité de l'information.

Les interfaces de la gestion des risques sont les suivantes :

- la gestion des risques de sécurité de l'information est partie intégrante de la gestion d'@RCHIMED ; à ce titre, ses résultats sont pris en compte dans la stratégie de la société ;
- l'ensemble de la société est concerné par la gestion des risques de sécurité de l'information, tant pour apprécier les risques que pour appliquer et faire appliquer des mesures de sécurité.

Exemple d'action type 1.1.3. Délimiter le périmètre de l'étude

Exemple

Le choix du périmètre d'étude s'est porté sur le sous-ensemble du système d'information du cabinet @RCHIMED correspondant à son cœur de métier :

- gestion des relations commerciales (gestion des devis, projets…) ;
- gestion des études (calculs de structure, plans techniques, visualisations 3D…) ;
- gestion des services web (nom de domaine, site Internet, courrier électronique…).

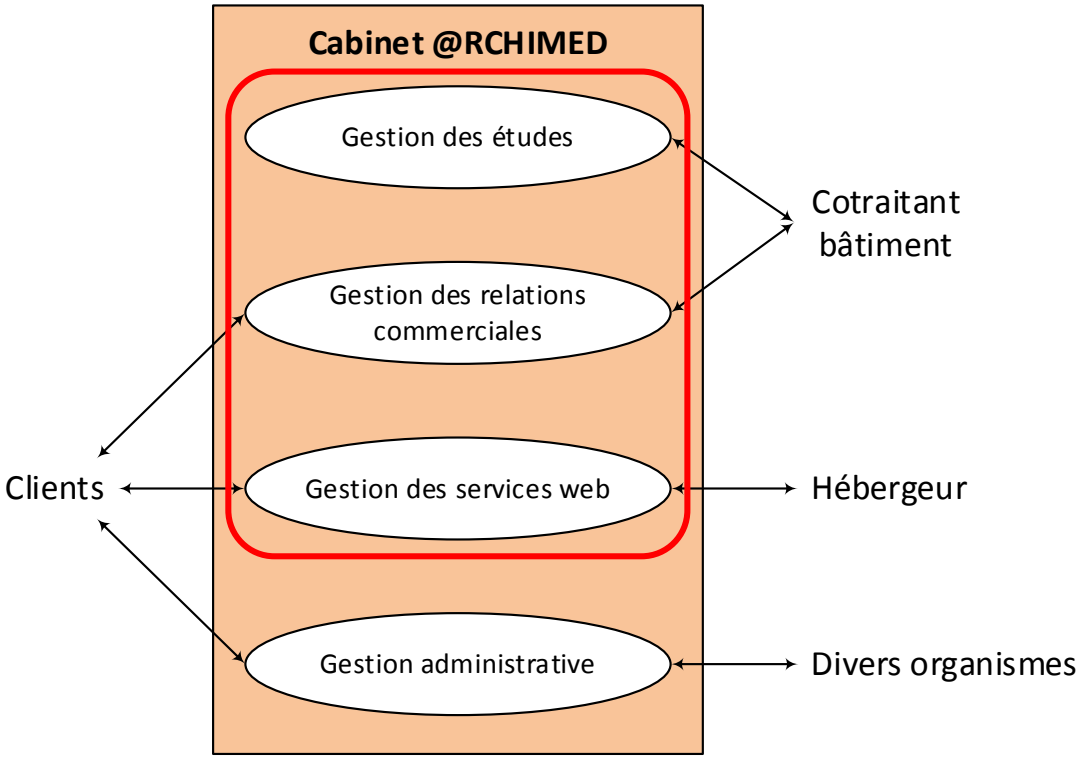


Figure 2 - ***Le périmètre d'étude***

La gestion administrative est donc en dehors du périmètre d'étude :

- gérer la comptabilité ;
- gérer les contentieux juridiques et techniques ;
- gestion administrative interne (ressources humaines, maintenance, assurances) ;
- gestion des permis de construire.

Les principales interfaces concernent :

- les clients (de visu, par téléphone, par courrier papier et électronique) ;
- les cotraitants bâtiment (de visu, par téléphone, par courrier papier et électronique) ;
- l'hébergeur du site web (via une connexion Internet, par courrier papier et électronique).

Le système informatique du cabinet @RCHIMED est composé de deux réseaux locaux, l'un pour le bureau d'études et l'autre pour le reste de la société, sur un seul site et dépendant uniquement de la société, utilisés par une douzaine de personnes manipulant des logiciels métiers.

La gestion du site web est assurée par un poste isolé, en relation avec un hébergeur sur Internet.

Le sujet de l'étude représente la partie du système d'information d'@RCHIMED indispensable pour qu'il exerce son métier. L'ensemble du patrimoine informationnel du cabinet est créé, traité et stocké sur ce système d'information.

Les enjeux suivants ont été identifiés :

- favoriser l'ouverture du système informatique vers l'extérieur ;
- démontrer la capacité du cabinet à protéger les projets sensibles (assurer la confidentialité relative aux aspects techniques…) ;
- améliorer les services rendus aux usagers et la qualité des prestations ;
- améliorer les échanges avec les autres organismes (fournisseurs, architectes).

Les participants à l'étude sont définis comme suit :

- la population à l'étude est l'ensemble des collaborateurs travaillant dans le périmètre choisi (gestion des relations commerciales, gestion des études et gestion des services web) ;
- au moins un personnel de chaque catégorie (direction, commercial, ingénieur, technicien) participe à l'étude ; d'autres personnels peuvent également participer à l'étude afin d'apporter un point de vue extérieur ;
- les critères de sélection sont les meilleures connaissances du métier en général, et des processus d'@RCHIMED.

Exemple d'action type 1.1.4. Identifier les paramètres à prendre en compte

Exemple

Un ensemble de contraintes à prendre en compte a été identifié :

- relatives au personnel :
  - le personnel est utilisateur de l'informatique, mais pas spécialiste,
  - le responsable informatique est l'adjoint du directeur, il est architecte de formation,
  - le personnel de nettoyage intervient de 7h à 8h,
  - la réception des clients se fait dans les bureaux des commerciaux, mais des visites ont parfois lieu au bureau d'études ;
- d'ordre calendaire :
  - la période de pointe se situant d'octobre à mai, toute action (installation de système de sécurité, formation et sensibilisation) se fera en dehors de cette période ;
  - d'ordre budgétaire :
  - la société a fait un effort important en matière d'informatisation, tout investissement supplémentaire devra être dûment justifié ;
- d'ordre technique :
  - les règles de conception architecturale doivent être respectées,
  - des logiciels professionnels du domaine architectural doivent être employés ;
- d'environnement :
  - le cabinet loue deux étages d'un immeuble au centre-ville,
  - le cabinet est au voisinage de commerces divers,
  - aucun déménagement n'est planifié

Exemple d'action type 1.1.5. Identifier les sources de menaces

Exemple

Le cabinet @RCHIMED souhaite s'opposer aux sources de menaces suivantes :

Types de sources de menaces	*Retenu ou non*	*Exemple*
Source humaine interne, malveillante, avec de faibles capacités	*Non, le cabinet n'estime pas y être exposé*	
Source humaine interne, malveillante, avec des capacités importantes	*Non, le cabinet n'estime pas y être exposé*	
Source humaine interne, malveillante, avec des capacités illimitées	*Non, le cabinet n'estime pas y être exposé*	
Source humaine externe, malveillante, avec de faibles capacités	*Oui*	✓ *Personnel de nettoyage (soudoyé)* ✓ *Script-kiddies*
Source humaine externe, malveillante, avec des capacités importantes	*Oui*	✓ *Concurrent (éventuellement en visite incognito)* ✓ *Maintenance informatique*
Source humaine externe, malveillante, avec des capacités illimitées	*Non, le cabinet n'estime pas y être exposé*	
Source humaine interne, sans intention de nuire, avec de faibles capacités	*Oui*	✓ *Employé peu sérieux*
Source humaine interne, sans intention de nuire, avec des capacités importantes	*Non, le cabinet n'estime pas y être exposé*	
Source humaine interne, sans intention de nuire, avec des capacités illimitées	*Oui*	✓ *Employé peu sérieux (ceux qui ont un rôle d'administrateur)*
Source humaine externe, sans intention de nuire, avec de faibles capacités	*Oui*	✓ *Client* ✓ *Cotraitant* ✓ *Partenaire*
Source humaine externe, sans intention de nuire, avec des capacités importantes	*Oui*	✓ *Fournisseur d'accès Internet* ✓ *Hébergeur*
Source humaine externe, sans intention de nuire, avec des capacités illimitées	*Non, le cabinet n'estime pas y être exposé*	
Virus non ciblé	*Oui*	✓ *Virus non ciblé*
Phénomène naturel	*Oui*	✓ *Phénomène naturel (foudre, usure…)*
Catastrophe naturelle ou sanitaire	*Oui*	✓ *Maladie*
Activité animale	*Non, le cabinet n'estime pas y être exposé*	
Événement interne	*Oui*	✓ *Panne électrique* ✓ *Incendie des locaux*

Exemple d'action type 1.2.1. Définir les critères de sécurité et élaborer les échelles de besoins

Exemple

Afin d'exprimer les besoins de sécurité, les critères de sécurité retenus sont les suivants :

Critères de sécurité	***Définitions***
Disponibilité	*Propriété d'accessibilité au moment voulu des biens essentiels.*
Intégrité	*Propriété d'exactitude et de complétude des biens essentiels.*
Confidentialité	*Propriété des biens essentiels de n'être accessibles qu'aux utilisateurs autorisés.*

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes de disponibilité :

Niveaux de l'échelle	***Description détaillée de l'échelle***
Plus de 72h	*Le bien essentiel peut être indisponible plus de 72 heures.*
Entre 24 et 72h	*Le bien essentiel doit être disponible dans les 72 heures.*
Entre 4 et 24h	*Le bien essentiel doit être disponible dans les 24 heures.*
Moins de 4h	*Le bien essentiel doit être disponible dans les 4 heures.*

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes d'intégrité :

Niveaux de l'échelle	***Description détaillée de l'échelle***
Détectable	*Le bien essentiel peut ne pas être intègre si l'altération est identifiée.*
Maîtrisé	*Le bien essentiel peut ne pas être intègre, si l'altération est identifiée et l'intégrité du bien essentiel retrouvée.*
Intègre	*Le bien essentiel doit être rigoureusement intègre.*

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes de confidentialité :

Niveaux de l'échelle	***Description détaillée de l'échelle***
Public	*Le bien essentiel est public.*
Limité	*Le bien essentiel ne doit être accessible qu'au personnel et aux partenaires.*
Réservé	*Le bien essentiel ne doit être accessible qu'au personnel (interne) impliquées.*
Privé	*Le bien essentiel ne doit être accessible qu'à des personnes identifiées et ayant le besoin d'en connaître.*

Exemple d'action type 1.2.2. Élaborer une échelle de niveau de gravité

L'échelle suivante sera utilisée pour estimer la gravité des événements redoutés et des risques :

Niveaux de l'échelle	***Description détaillée de l'échelle***
1. Négligeable	*@RCHIMED surmontera les impacts sans aucune difficulté.*
2. Limitée	*@RCHIMED surmontera les impacts malgré quelques difficultés.*
3. Importante	*@RCHIMED surmontera les impacts avec de sérieuses difficultés.*
4. Critique	*@RCHIMED ne surmontera pas les impacts (sa survie est menacée).*

Exemple d'action type 1.2.3. Élaborer une échelle de niveau de vraisemblance

Exemple

L'échelle suivante sera utilisée pour estimer la vraisemblance des scénarios de menaces et des risques :

Niveaux de l'échelle	*Description détaillée de l'échelle*
1. Minime	*Cela ne devrait pas se (re)produire.*
2. Significative	*Cela pourrait se (re)produire.*
3. Forte	*Cela devrait se (re)produire un jour ou l'autre.*
4. Maximale	*Cela va certainement se (re)produire prochainement.*

Exemple d'action type 1.2.4. Définir les critères de gestion des risques

Exemple

Les critères de gestion des risques retenus sont les suivants :

Action	*Critère de gestion des risques (règle choisie pour réaliser l'action)*
Estimation des événements redoutés (module 2)	✓ *Les événements redoutés sont estimés en termes de gravité à l'aide de l'échelle définie à cet effet.*
Évaluation des événements redoutés (module 2)	✓ *Les événements redoutés sont classés par ordre décroissant de vraisemblance.*
Estimation des risques (module 4)	✓ *La gravité d'un risque est égale à celle de l'événement redouté considéré.* ✓ *La vraisemblance d'un risque est égale à la vraisemblance maximale de tous les scénarios de menaces liés à l'événement redouté considéré.*
Évaluation des risques (module 4)	✓ *Les risques dont la gravité est critique, et ceux dont la gravité est importante et la vraisemblance forte ou maximale, sont jugés comme intolérables.* ✓ *Les risques dont la gravité est importante et la vraisemblance significative, et ceux dont la gravité est limitée et la vraisemblance forte ou maximale sont jugés comme significatifs.* ✓ *Les autres risques sont jugés comme négligeables.*
…	*…*

Exemple d'action type 1.3.1. Identifier les biens essentiels, leurs relations et leurs dépositaires

Exemple

Dans le cadre du sujet d'étude, le cabinet @RCHIMED a retenu les processus suivants en tant que biens essentiels :

Processus essentiels	***Informations essentielles concernées***	***Dépositaires***
Établir les devis (estimation du coût global d'un projet, négociations avec les clients…)	✓ *Cahier des charges* ✓ *Catalogues techniques* ✓ *Contrat (demande de réalisation)* ✓ *Devis*	*Service commercial*
Créer des plans et calculer les structures	✓ *Dossier technique d'un projet* ✓ *Paramètres techniques (pour les calculs de structure)* ✓ *Plan technique* ✓ *Résultat de calcul de structure*	*Bureau d'études*
Créer des visualisations	✓ *Dossier technique d'un projet* ✓ *Visualisation 3D*	*Bureau d'études*
Gérer le contenu du site Internet	✓ *Informations société (contacts, Présentation, …)* ✓ *Exemple de devis* ✓ *Exemple de visualisation 3D* ✓ *Page Web*	*Directeur adjoint*

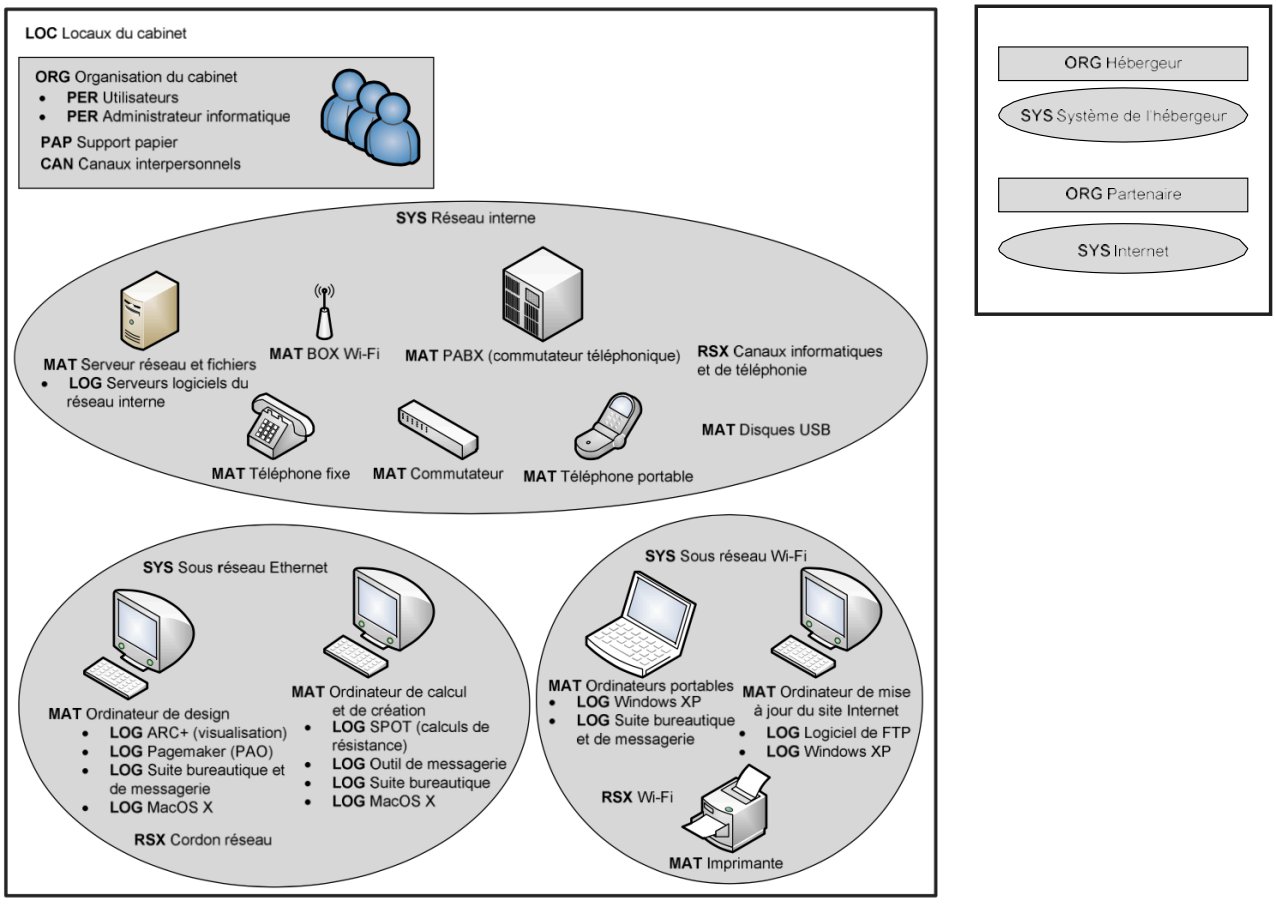
Exemple d'action type 1.3.2. Identifier les biens supports, leurs relations et leurs propriétaires

Exemple

Sans les détailler dans un premier temps, @RCHIMED a retenu les biens supports suivants :

- en interne :
  - SYS – Réseau interne,
  - SYS – Sous réseau Ethernet,
  - SYS – Sous réseau Wifi,
  - ORG – Organisation du cabinet,
  - LOC – Locaux du cabinet ;
- en interface :
  - SYS – Système de l'hébergeur (Internet et par courrier électronique),
  - ORG – Hébergeur (par courrier papier),
  - SYS – Internet (pour des accès distants et le courrier électronique),
  - ORG – Partenaire (cotraitants bâtiment, clients, …).

Le schéma suivant décompose ces biens supports et les positionne les uns par rapport aux autres :



Exemple d'action type 1.3.3. Déterminer le lien entre les biens essentiels et les biens supports

Exemple

Le tableau suivant présente les biens supports et leurs liens avec les biens essentiels :

Biens essentiels / ***Biens supports***	***Établir les devis***	***Créer des plans et calculer les structures***	***Créer des visualisations***	***Gérer le contenu du site Internet***
Biens supports communs à @RCHIMED				
SYS – Réseau interne	*X*	*X*	*X*	*X*
MAT – Serveur réseau et fichiers	*X*	*X*	*X*	*X*
LOG – Serveurs logiciels du réseau interne		*X*	*X*	
MAT – Disque USB	*X*	*X*	*X*	
MAT – BOX Wifi	*X*	*X*	*X*	*X*
MAT – Commutateur	*X*	*X*	*X*	*X*
MAT – PABX (commutateur téléphonique)	*X*	*X*	*X*	*X*
MAT – Téléphone fixe	*X*	*X*	*X*	*X*
MAT – Téléphone portable	*X*	*X*	*X*	*X*
RSX – Canaux informatiques et de téléphonie	*X*	*X*	*X*	*X*
ORG – Organisation du cabinet	*X*	*X*	*X*	*X*
PER – Utilisateur	*X*	*X*	*X*	
PER – Administrateur informatique	*X*	*X*	*X*	*X*
PAP – Support papier	*X*	*X*	*X*	
CAN – Canaux interpersonnels	*X*	*X*	*X*	*X*
LOC – Locaux du cabinet	*X*	*X*	*X*	*X*
Biens supports spécifiques au bureau d'études				
SYS – Sous réseau Ethernet		*X*	*X*	
MAT – Ordinateur de design		*X*	*X*	
LOG – MacOS X		*X*	*X*	
LOG – ARC+ (visualisation)			*X*	
LOG – Pagemaker (PAO)		*X*	*X*	
LOG – Suite bureautique et de messagerie		*X*	*X*	
MAT – Ordinateur de calcul et de création		*X*		
…	*…*	*…*	*…*	*…*

Exemple d'action type 1.3.4. Identifier les mesures de sécurité existantes

Exemple

@RCHIMED a recensé les mesures de sécurité existantes suivantes :

Mesure de sécurité	*Bien support sur lequel elle repose*	*Thème ISO 27002*	*Prévention*	*Protection*	*Récupération*
Accord sur le niveau de service de l'hébergeur	*ORG – Organisation du cabinet*	*6.2. Tiers*	*X*		*X*
Activation d'une alarme anti-intrusion durant les heures de fermeture	*LOC – Locaux du cabinet*	*9.1. Zones sécurisées*	*X*		
Consignes de fermeture à clef des locaux	*LOC – Locaux du cabinet*	*9.1. Zones sécurisées*		*X*	
Dispositifs de lutte contre l'incendie	*LOC – Locaux du cabinet*	*9.1. Zones sécurisées*		*X*	
Climatisation	*LOC – Locaux du cabinet*	*9.2. Sécurité du matériel*	*X*		
Contrat de maintenance informatique (intervention sous 4h)	*ORG – Organisation du cabinet*	*9.2. Sécurité du matériel*	*X*		*X*
Alimentation secourue	*MAT – Serveur réseau et fichiers*	*9.2. Sécurité du matériel*		*X*	
Installation d'un antivirus sous Windows XP	*LOG – Windows XP*	*10.4. Protection contre les codes malveillant et mobile*		*X*	
Sauvegarde hebdomadaire sur des disques USB stockés dans une armoire fermant à clef	*MAT – Disque USB*	*10.5. Sauvegarde*			*X*
Activation du WPA2	*MAT – Commutateur*	*10.6. Gestion de la sécurité des*	*X*		
Accès restreint en entrée (messagerie, services WEB…)	*MAT – Commutateur*	*10.6. Gestion de la sécurité des réseaux*	*X*		
Contrôle d'accès par mot de passe sous Windows XP	*LOG – Windows XP*	*11.5. Contrôle d'accès au système d'exploitation*	*X*		
Assurance multirisque professionnelle et sur les matériels informatiques	*ORG – Organisation du cabinet*	*14.1. Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité*			*X*
…	*…*	*…*	*…*	*…*	*…*

Exemple d'action type 2.1.1. Analyser tous les événements redoutés

Exemple

Chaque ligne du tableau suivant représente un événement redouté par le cabinet @RCHIMED (bien essentiel, critère de sécurité, besoin de sécurité selon les échelles de besoin, sources de menaces et impacts). La gravité de chaque évènement redouté est estimée (cf. échelle de gravité) sans tenir compte des mesures de sécurité existantes.

Événement redouté	*Besoin de sécurité*	*Sources de menaces*	*Impacts*	*Gravité*
Établir les devis				
Indisponibilité de devis	*24-72h*	✓ *Employé peu sérieux* ✓ *Incendie des locaux* ✓ *Panne électrique*	✓ *Impossibilité de signer un contrat* ✓ *Perte d'un marché* ✓ *Perte de crédibilité*	*2. Limitée*
Altération de devis	*Intègre*	✓ *Employé peu sérieux*	✓ *Impossibilité de signer un contrat* ✓ *Perte d'un marché* ✓ *Impossibilité de remplir les obligations légales* ✓ *Perte de crédibilité*	*3. Importante*
Compromission de devis	*Limité*	✓ *Employé peu sérieux* ✓ *Concurrent*	✓ *Perte d'un marché* ✓ *Action en justice à l'encontre du cabinet* ✓ *Perte de crédibilité*	*3. Importante*
Créer des plans et calculer les structures				
Indisponibilité de plans ou de calculs de structures	*24-72h*	✓ *Employé peu sérieux* ✓ *Virus non ciblé* ✓ *Personnel de nettoyage (soudoyé)* ✓ *Personnels de maintenance* ✓ *Panne électrique*	✓ *Perte de crédibilité*	*2. Limitée*
Altération de plans ou de calculs de structures	*Intègre*	✓ *Employé peu sérieux* ✓ *Concurrent*	✓ *Impossibilité de remplir les obligations légales* ✓ *Perte de crédibilité* ✓ *Action en justice à l'encontre du cabinet* ✓ *Perte de notoriété* ✓ *Mise en danger (bâtiment qui s'écroule)*	*4. Critique*
Compromission de plans ou calculs de structures	*Limité*	✓ *Employé peu sérieux* ✓ *Personnel de nettoyage (soudoyé)* ✓ *Personnels de maintenance*	✓ *Perte d'un marché* ✓ *Perte de crédibilité* ✓ *Perte de notoriété* ✓ *Impossibilité de remplir les obligations légales (si contractuel)*	*3. Importante*
Créer des visualisations				
Indisponibilité de visualisations	*24-72h*	✓ *Employé peu sérieux* ✓ *Virus non ciblé* ✓ *Incendie des locaux* ✓ *Panne électrique*	✓ *Bouche à oreille négatif* ✓ *Perte de crédibilité* ✓ *Perte de notoriété*	*2. Limitée*
Altération de visualisations	*Détectable*	✓ *Employé peu sérieux*	✓ *Bouche à oreille négatif* ✓ *Perte de crédibilité* ✓ *Perte de notoriété*	*2. Limitée*
Compromission de visualisations	*Public*	-	-	*1. Négligeable*
Gérer le contenu du site Internet				
Indisponibilité du site Internet	*24-72h*	✓ *Employé peu sérieux* ✓ *Virus non ciblé* ✓ *Concurrent* ✓ *Script-kiddies* ✓ *Panne électrique* ✓ *Hébergeur*	✓ *Perte de crédibilité* ✓ *Perte de notoriété* ✓ *Bouche à oreille négatif*	*2. Limitée*
Altération du contenu du site Internet	*Maîtrisé*	✓ *Employé peu sérieux* ✓ *Virus non ciblé* ✓ *Concurrent* ✓ *Script-kiddies* ✓ *Hébergeur*	✓ *Perte de crédibilité* ✓ *Perte de notoriété* ✓ *Bouche à oreille négatif* ✓ *Perte d'un marché ou de clientèle*	*3. Importante*
Compromission du contenu du site Internet	*Public*	-	-	*1. Négligeable*

Exemple d'action type 2.1.2. Évaluer chaque événement redouté

Exemple

L'importance relative des événements redoutés précédemment analysés (identifiés et estimés) est évaluée à l'aide du tableau suivant (cf. critères de gestion des risques) :

Gravité	*Événements redoutés*
4. Critique	✓ *Altération de plans ou de calculs de structures*
3. Importante	✓ *Altération de devis* ✓ *Compromission de plans ou calculs de structures* ✓ *Compromission de devis* ✓ *Altération du contenu du site Internet*
2. Limitée	✓ *Indisponibilité de devis* ✓ *Indisponibilité de visualisations* ✓ *Altération de visualisations* ✓ *Indisponibilité de plans ou de calculs de structures* ✓ *Indisponibilité du site Internet*
1. Négligeable	✓ *Compromission de visualisations Compromission du contenu du site* ✓ *Internet*

Exemple d'action type 3.1.1. Analyser tous les scénarios de menaces

Exemple

Les pages suivantes présentent les scénarios de menaces potentiellement réalisables dans le cadre du sujet de l'étude.

Les sources de menaces susceptibles d'en être à l'origine sont identifiées et la vraisemblance de chaque scénario de menace est estimée (cf. échelle de vraisemblance).

Le détail des scénarios de menaces (menaces, vulnérabilités et prérequis) est décrit dans les bases de connaissances de la méthode EBIOS.

Scénarios de menaces	*Sources de menaces*	*Vraisemblance*
SYS – Réseau interne		
Menaces sur le réseau interne causant une indisponibilité	√ *Employé peu sérieux* √ *Maintenance informatique* √ *Script-kiddies* √ *Virus non ciblé* √ *Incendie des locaux* √ *Panne électrique* √ *Phénomène naturel (foudre, usure…)*	*3. Forte*
Menaces sur le réseau interne causant une altération	√ *Employé peu sérieux* √ *Maintenance informatique* √ *Script-kiddies* √ *Virus non ciblé*	*2. Significative*
Menaces sur le réseau interne causant une compromission	√ *Employé peu sérieux* √ *Maintenance informatique* √ *Script-kiddies*	*2. Significative*
SYS – Sous réseau Ethernet		
Menaces sur le sous réseau Ethernet causant une indisponibilité	√ *Employé peu sérieux* √ *Maintenance informatique* √ *Script-kiddies* √ *Virus non ciblé* √ *Incendie des locaux* √ *Panne électrique* √ *Phénomène naturel (foudre, usure…)*	*3. Forte*
Menaces sur le sous réseau Ethernet causant une altération	√ *Employé peu sérieux* √ *Maintenance informatique* √ *Script-kiddies* √ *Virus non ciblé*	*2. Significative*
Menaces sur le sous réseau Ethernet causant une compromission	√ *Employé peu sérieux* √ *Maintenance informatique* √ *Script-kiddies*	*2. Significative*
SYS – Sous réseau Wifi		
Menaces sur le sous réseau Wifi causant une indisponibilité	√ *Employé peu sérieux* √ *Maintenance informatique* √ *Script-kiddies* √ *Virus non ciblé* √ *Incendie des locaux* √ *Panne électrique* √ *Phénomène naturel (foudre, usure…)*	*3. Forte*
Menaces sur le sous réseau Wifi causant une altération	√ *Employé peu sérieux* √ *Maintenance informatique* √ *Script-kiddies* √ *Virus non ciblé*	*3. Forte*
Menaces sur le sous réseau Wifi causant une compromission	√ *Employé peu sérieux* √ *Maintenance informatique* √ *Script-kiddies*	*3. Forte*
ORG – Organisation du cabinet		
Menaces sur l'organisation d'@RCHIMED causant une indisponibilité	√ *Employé peu sérieux* √ *Personnel de nettoyage* √ *Maladie*	*2. Significative*
Menaces sur l'organisation d'@RCHIMED causant une altération	√ *Employé peu sérieux Personnel de nettoyage*	*1. Minime*
Menaces sur l'organisation d'@RCHIMED causant une compromission	√ *Concurrent (en visite incognito)* √ *Employé peu sérieux* √ *Cotraitant* √ *Client* √ *Maintenance informatique* √ *Personnel de nettoyage*	*4. Maximale*

Scénarios de menaces	Sources de menaces	Vraisemblance
SYS – Système de l'hébergeur		
Menaces sur le système de l'hébergeur causant une indisponibilité	√ *Hébergeur* √ *Script-kiddies* √ *Virus non ciblé* √ *Panne électrique* √ *Phénomène naturel (foudre, usure…)*	*4. Maximale*
Menaces sur le système de l'hébergeur causant une altération	√ *Hébergeur* √ *Script-kiddies* √ *Virus non ciblé*	*3. Forte*
Menaces sur le système de l'hébergeur causant une compromission	√ *Concurrent* √ *Client* √ *Partenaire*	*4. Maximale*
ORG – Hébergeur		
Menaces sur l'hébergeur causant une indisponibilité	√ *Hébergeur*	*2. Significative*
Menaces sur l'hébergeur causant une altération	√ *Hébergeur*	*2. Significative*
Menaces sur l'hébergeur causant une compromission	√ *Hébergeur*	*1. Minime*
SYS – Internet		
Menaces sur Internet causant une indisponibilité	√ *Fournisseur d'accès Internet*	*2. Significative*
Menaces sur Internet causant une altération	√ *Script-kiddies*	*1. Minime*
Menaces sur Internet causant une compromission	√ *Script-kiddies* √ *Concurrent*	*2. Significative*
ORG – Partenaire		
Menaces sur un partenaire causant une indisponibilité	√ *Partenaire*	*3. Forte*
Menaces sur un partenaire causant une altération	√ *Partenaire*	*1. Minime*
Menaces sur un partenaire causant une compromission	√ *Partenaire*	*4. Maximale*

Exemple d'action type 3.1.2. Évaluer chaque scénario de menace

Exemple

L'importance relative des scénarios de menaces précédemment analysés (identifiés et estimés) est évaluée de la façon suivante (cf. critères de gestion des risques) :

Vraisemblance	*Scénarios de menaces*
4. Maximale	✓ *Menaces sur l'organisation d'@RCHIMED causant une compromission* ✓ *Menaces sur le système de l'hébergeur causant une indisponibilité* ✓ *Menaces sur le système de l'hébergeur causant une compromission* ✓ *Menaces sur un partenaire causant une compromission*
3. Forte	✓ *Menaces sur le réseau interne causant une indisponibilité* ✓ *Menaces sur le sous réseau Ethernet causant une indisponibilité* ✓ *Menaces sur le sous réseau Wifi causant une indisponibilité* ✓ *Menaces sur le sous réseau Wifi causant une altération* ✓ *Menaces sur le sous réseau Wifi causant une compromission* ✓ *Menaces sur le système de l'hébergeur causant une altération* ✓ *Menaces sur un partenaire causant une indisponibilité*
2. Significative	✓ *Menaces sur le réseau interne causant une altération* ✓ *Menaces sur le réseau interne causant une compromission* ✓ *Menaces sur le sous réseau Ethernet causant une altération* ✓ *Menaces sur le sous réseau Ethernet causant une compromission* ✓ *Menaces sur l'organisation d'@RCHIMED causant une indisponibilité* ✓ *Menaces sur l'hébergeur causant une indisponibilité* ✓ *Menaces sur l'hébergeur causant une altération* ✓ *Menaces sur Internet causant une indisponibilité* ✓ *Menaces sur Internet causant une compromission*
1. Minime	✓ *Menaces sur l'organisation d'@RCHIMED causant une altération* ✓ *Menaces sur l'hébergeur causant une compromission* ✓ *Menaces sur Internet causant une altération* ✓ *Menaces sur un partenaire causant une altération*

Exemple d'action type 4.1.1. Analyser les risques

Exemple

@RCHIMED a établi la liste des risques à partir des événements redoutés et des scénarios de menaces précédemment appréciés.

Les mesures de sécurité existantes ayant un effet sur chaque risque ont également été identifiées.

La gravité et la vraisemblance ont finalement été estimées, sans, puis avec, les mesures de sécurité (les niveaux rayés correspondent aux valeurs avant application de ces mesures).

Risque lié à l'indisponibilité d'un devis au-delà de 72h

Événement redouté	*Besoin de sécurité*	*Sources de menaces*	*Impacts*	*Gravité*
Indisponibilité de devis	*24-72h*	√ *Employé peu sérieux* √ *Incendie des locaux* √ *Panne électrique*	√ *Impossibilité de signer un contrat* √ *Perte d'un marché* √ *Perte de crédibilité*	*2. Limitée*

Scénarios de menaces	*Sources de menaces*	*Vraisemblance*
Menaces sur le réseau interne causant une indisponibilité	√ *Employé peu sérieux* √ *Maintenance informatique* √ *Script-kiddies* √ *Virus non ciblé* √ *Incendie des locaux Panne électrique* √ *Phénomène naturel (foudre, usure…)*	*3. Forte*
Menaces sur le sous réseau Wifi causant une indisponibilité	√ *Employé peu sérieux* √ *Maintenance informatique* √ *Script-kiddies* √ *Virus non ciblé* √ *Incendie des locaux* √ *Panne électrique* √ *Phénomène naturel (foudre, usure…)*	*3. Forte*
Menaces sur l'organisation d'@RCHIMED causant une indisponibilité	√ *Employé peu sérieux* √ *Personnel de nettoyage* √ *Maladie*	*2. Significative*
Menaces sur Internet causant une indisponibilité	√ *Fournisseur d'accès Internet*	*2. Significative*
Menaces sur un partenaire causant une indisponibilité	√ *Partenaire*	*3. Forte*

Mesure de sécurité existante	*Bien support sur lequel elle repose*	*Prévention*	*Protection*	*Récupération*
Activation du WPA2	*MAT – Commutateur*	*X*		
Assurance multirisque professionnelle et sur les matériels informatiques	*ORG – Organisation du cabinet*			*X*
Climatisation	*LOC – Locaux du cabinet*	*X*		
Contrat de maintenance informatique (intervention sous 4h)	*ORG – Organisation du cabinet*	*X*		*X*
Contrôle d'accès par mot de passe	*LOG – Windows XP*	*X*		
Dispositifs de lutte contre l'incendie	*LOC – Locaux du cabinet*		*X*	
Installation d'un antivirus	*LOG – Windows XP*		*X*	
Alimentation secourue	*MAT – Serveur réseau et fichiers*		*X*	
Accès restreint en entrée (messagerie, services WEB…)	*MAT – Commutateur*	*X*		
Sauvegarde hebdomadaire sur des disques USB stockés dans une armoire fermant à clef	*MAT – Disque USB*			*X*

Niveau de risque				
Gravité	*1. Négligeable*	***2. Limitée***	*3. Importante*	*4. Critique*
Vraisemblance	*1. Minime*	***2. Significative***	~~*3. Forte*~~	*4. Maximale*

Risque lié à l'altération d'un devis qui doit rester rigoureusement intègre […]

Risque lié à la compromission d'un devis au-delà du personnel et des partenaires […]

Exemple d'action type 4.1.2. Évaluer les risques

Exemple

Les risques précédemment analysés (identifiés et estimés) peuvent être évalués à l'aide du tableau suivant (les risques rayés correspondent à ceux réduits par des mesures de sécurité existantes) :

Gravité					
	4. Critique		✓ *Risque lié à l'altération de plans ou de calculs de structures qui doivent rester*		
	3. Importante		✓ *Risque lié à l'altération du contenu du site Internet sans pouvoir la détecter ni la retrouver*	✓ *Risque lié à l'altération d'un devis qui doit rester rigoureusement intègre* ✓ ~~*Risque lié à l'altération du contenu du site Internet sans pouvoir la détecter ni la retrouver*~~	✓ *Risque lié à la compromission d'un devis au-delà du personnel et des partenaires* ✓ *Risque lié à la compromission de plans ou calculs de structures au-delà des personnels et partenaires*
	2. Limitée		✓ *Risque lié à l'indisponibilité d'un devis au-delà de 72h* ✓ *Risque lié à l'indisponibilité de plans ou de calculs de structures au-delà de 72h* ✓ *Risque lié à l'indisponibilité de visualisations au-delà de 72h* ✓ *Risque lié à l'indisponibilité du contenu du site Internet au-delà de 72h*	✓ ~~*Risque lié à l'indisponibilité d'un devis au-delà de 72h*~~ ✓ ~~*Risque lié à l'indisponibilité de plans ou de calculs de structures au-delà de 72h*~~ ✓ ~~*Risque lié à l'indisponibilité de visualisations au-delà de 72h*~~ ✓ *Risque lié à l'altération de visualisations sans pouvoir la détecter*	✓ ~~*Risque lié à l'indisponibilité du contenu du site Internet au-delà de 72h*~~
	1. Négligeable				✓ *Risque lié à la compromission de visualisations, jugées comme publiques* ✓ *Risque lié à la compromission du contenu du site Internet public*
		1. Minime	***2. Significative***	***3. Forte***	***4. Maximale***
		Vraisemblance			

Risques négligeables	*Risques significatifs*	*Risques intolérables*

Exemple d'action type 4.2.1. Choisir les options de traitement des risques

Exemple

@RCHIMED souhaite essentiellement réduire les risques jugés comme prioritaires et significatifs, et prendre les risques jugés comme non prioritaires.

Le tableau suivant présente les objectifs de sécurité identifiés (les croix correspondent aux premiers choix, les croix entre parenthèses correspondent aux autres possibilités acceptées) :

Risque	*Évitement*	*Réduction*	*Prise*	*Transfert*
Risque lié à l'indisponibilité d'un devis au-delà de 72h		*(X)*	*X*	
Risque lié à l'altération d'un devis qui doit rester rigoureusement intègre	*(X)*	*X*	*X*	*(X)*
Risque lié à la compromission d'un devis au-delà du personnel et des partenaires	*(X)*	*X*	*X*	*(X)*
Risque lié à l'indisponibilité de plans ou de calculs de structures au-delà de 72h		*(X)*	*X*	
Risque lié à l'altération de plans ou de calculs de structures qui doivent rester rigoureusement intègres	*(X)*	*X*	*X*	*(X)*
Risque lié à la compromission de plans ou calculs de structures au-delà des personnels et partenaires	*(X)*	*X*	*X*	*(X)*
Risque lié à l'indisponibilité de visualisations au-delà de 72h		*(X)*	*X*	
Risque lié à l'altération de visualisations sans pouvoir la détecter		*X*	*(X)*	*(X)*
Risque lié à la compromission de visualisations, jugées comme publiques		*(X)*	*X*	
Risque lié à l'indisponibilité du contenu du site Internet au-delà de 72h		*(X)*	*X*	
Risque lié à l'altération du contenu du site Internet sans pouvoir la détecter ni la retrouver		*X*	*(X)*	*(X)*
Risque lié à la compromission du contenu du site Internet public		*(X)*	*X*	

Exemple d'action type 4.2.2. Analyser les risques résiduels

Exemple

À l'issue de l'identification des objectifs de sécurité, @RCHIMED a mis en évidence les risques résiduels suivants :

Risques résiduels	*Gravité*	*Vraisemblance*
Risque lié à l'indisponibilité d'un devis au-delà de 72h	*2. Limitée*	*2. Significative*
Risque lié à l'indisponibilité de plans ou de calculs de structures au-delà de 72h	*2. Limitée*	*2. Significative*
Risque lié à l'indisponibilité de visualisations au-delà de 72h	*2. Limitée*	*2. Significative*
Risque lié à la compromission de visualisations, jugées comme publiques	*1. Négligeable*	*4. Maximale*
Risque lié à l'indisponibilité du contenu du site Internet au-delà de 72h	*2. Limitée*	*2. Significative*
Risque lié à la compromission du contenu du site Internet public	*1. Négligeable*	*4. Maximale*

On note que ces risques résiduels pourront être réduits ultérieurement, quand les autres risques seront devenus acceptables.

Exemple d'action type 5.1.1. Déterminer les mesures de sécurité

Exemple

Le tableau suivant présente la liste des mesures de sécurité destinées à réduire ou transférer les risques prioritaires (elles traitent également les autres risques) :

Mesure de sécurité	*R1*	*R2*	*R3*	*R4*	*R5*	*R6*	*Bien support sur lequel elle repose*	*Thème ISO 27002*	*Prévention*	*Protection*	*Récupération*
Chiffrement des fichiers liés aux plans et calculs de structures à l'aide de certificats électroniques				*X*			*LOG – MacOS X*	*7.1. Responsabilités relatives aux biens*		*X*	
Désactivation des composants inutiles sur le serveur	*X*	*X*	*X*	*X*	*X*	*X*	*LOG – Serveurs logiciels du réseau interne*	*10.1. Procédures et responsabilités liées à l'exploitation*	*X*		
Mise à jour régulière de l'antivirus des serveurs et de sa base de signatures	*X*		*X*		*X*	*X*	*LOG – Windows XP*	*10.4. Protection contre les codes malveillant et mobile*		*X*	
Accès restreint en entrée (messagerie, services WEB…)	*X*	*X*	*X*	*X*	*X*	*X*	*MAT – Commutateur*	*10.6. Gestion de la sécurité des réseaux*	*X*		
Rangement des supports amovibles dans un meuble fermant à clef		*X*		*X*			*MAT – Disque USB*	*10.7. Manipulation des supports*	*X*		
Utilisation d'antivols pour les ordinateurs portables		*X*		*X*			*MAT – Ordinateurs portables*	*9.2. Sécurité du matériel*	*X*		*X*
Utilisation de films empêchant l'espionnage de l'écran des ordinateurs portables		*X*		*X*			*MAT – Ordinateurs portables*	*9.2. Sécurité du matériel*	*X*		*X*
Accompagnement systématique des visiteurs dans les locaux		*X*		*X*			*ORG – Organisation du cabinet*	*6.2. Tiers*	*X*	*X*	
Inventaire des biens sensibles	*X*	*X*	*X*	*X*	*X*	*X*	*ORG – Organisation du cabinet*	*7.1. Responsabilités relatives aux biens*	*X*	*X*	*X*
Accord sur le niveau de service de l'hébergeur						*X*	*ORG – Organisation du cabinet*	*10.2. Gestion de la prestation de service par un tiers*	*X*		*X*
Contrôle annuel de l'application des mesures de sécurité	*X*	*X*	*X*	*X*	*X*	*X*	*ORG – Organisation du cabinet*	*15.3. Prises en compte de l'audit du système d'information*	*X*		
Assurance multirisque professionnelle et sur les matériels informatiques		*X*					*ORG – Organisation du cabinet*	*14.1. Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité*			*X*
Destruction des documents sensibles lors de leur mise au rebut		*X*		*X*			*PAP – Support papier*	*10.7. Manipulation des supports*	*X*		
Sensibilisation régulière des personnels aux risques encourus	*X*	*X*	*X*	*X*	*X*	*X*	*PER – Utilisateur*	*8.2. Pendant la durée du contrat*	*X*		
Retrait des droits d'accès en fin de contrat	*X*	*X*	*X*	*X*	*X*	*X*	*PER – Administrateur*	*8.3. Fin ou modification de contrat*	*X*		
Utilisation de mots de passe de qualité pour chaque compte utilisateur	*X*	*X*	*X*	*X*	*X*		*PER – Utilisateur*	*11.3. Responsabilités utilisateurs*	*X*		
…	*…*	*…*	*…*	*…*	*…*	*…*	*…*	*…*	*…*	*…*	*…*

Ces mesures de sécurité ont été déterminées dans l'objectif de couvrir différents éléments des risques à traiter (vulnérabilités, menaces, sources de menaces, besoins de sécurité ou impacts), d'aborder la plupart des thèmes de l'ISO 27002, de couvrir les différentes lignes de défense (prévention, protection et récupération), et ont été optimisées bien support par bien support.

Exemple d'action type 5.1.2. Analyser les risques résiduels

Exemple

Si les mesures de sécurité précédemment identifiées sont mises en œuvre, alors le niveau des risques jugés comme intolérables ou significatifs peut être ré-estimé comme suit :

Risque lié à l'altération d'un devis qui doit rester rigoureusement intègre

Niveau de risque				
Gravité	*1. Négligeable*	*2. Limitée*	***3. Importante***	*4. Critique*
Vraisemblance	***1. Minime***	~~*2. Significative*~~	~~*3. Forte*~~	*4. Maximale*

Risque lié à la compromission d'un devis au-delà du personnel et des partenaires

Niveau de risque				
Gravité	*1. Négligeable*	***2. Limitée***	~~*3. Importante*~~	*4. Critique*
Vraisemblance	*1. Minime*	***2. Significative***	~~*3. Forte*~~	~~*4. Maximale*~~

Risque lié à l'altération de plans ou de calculs de structures qui doivent rester rigoureusement intègres

Niveau de risque				
Gravité	*1. Négligeable*	*2. Limitée*	***3. Importante***	~~*4. Critique*~~
Vraisemblance	***1. Minime***	~~*2. Significative*~~	*3. Forte*	*4. Maximale*

Risque lié à la compromission de plans ou calculs de structures au-delà des personnels et partenaires

Niveau de risque				
Gravité	*1. Négligeable*	***2. Limitée***	~~*3. Importante*~~	*4. Critique*
Vraisemblance	*1. Minime*	***2. Significative***	~~*3. Forte*~~	~~*4. Maximale*~~

Exemple d’action type 5.1.3. Établir une déclaration d'applicabilité

Exemple

La prise en compte de chaque contrainte identifiée est explicitée comme suit :

Paramètre à prendre en compte	***Explication / Justification***
Le personnel est utilisateur de l'informatique, mais pas spécialiste	***Pris en compte*** *Les mesures de sécurité applicables par le personnel ne demandent pas une grande expertise*
Le personnel de nettoyage intervient de 7h à 8h	***Non pris en compte*** *Les horaires doivent correspondre à ceux du personnel*
Aucun déménagement n'est planifié	***Pris en compte*** *Les mesures de sécurité formalisées ne demandent pas de déménagement*
…	*…*

Exemple d'action type 5.2.1. Élaborer le plan d'action et suivre la réalisation des mesures de sécurité

Exemple

Le plan d'action d'@RCHIMED, trié par terme, avancement et coût financier, est établi comme suit :

Mesure de sécurité	Responsable	Difficulté	Coût financier	Terme	Avancement
Mesures du trimestre					
Activation d'une alarme anti-intrusion durant les heures de fermeture	*Directeur*	*1. Faible*	*1. Nul*	*1. Trimestre*	*3. Terminé*
Consignes de fermeture à clef des locaux	*Directeur*	*1. Faible*	*1. Nul*	*1. Trimestre*	*3. Terminé*
Dispositifs de lutte contre l'incendie	*Directeur adjoint*	*1. Faible*	*1. Nul*	*1. Trimestre*	*3. Terminé*
Climatisation	*Directeur adjoint*	*1. Faible*	*1. Nul*	*1. Trimestre*	*3. Terminé*
Contrôle d'accès par mot de passe sous MacOS X	*Directeur adjoint*	*1. Faible*	*1. Nul*	*1. Trimestre*	*3. Terminé*
Contrôle d'accès par mot de passe sous Windows XP	*Directeur adjoint*	*1. Faible*	*1. Nul*	*1. Trimestre*	*3. Terminé*
Accès restreint en entrée (messagerie, services WEB…)	*Directeur adjoint*	*1. Faible*	*1. Nul*	*1. Trimestre*	*3. Terminé*
Activation du WPA2	*Directeur adjoint*	*1. Faible*	*1. Nul*	*1. Trimestre*	*3. Terminé*
Sauvegarde hebdomadaire sur des disques USB stockés dans un meuble fermant à clef	*Directeur adjoint*	*1. Faible*	*1. Nul*	*1. Trimestre*	*3. Terminé*
Installation d'un antivirus sous MacOS X	*Directeur adjoint*	*1. Faible*	*2. Moins de 1000€*	*1. Trimestre*	*3. Terminé*
Installation d'un antivirus sous Windows XP	*Directeur adjoint*	*1. Faible*	*2. Moins de 1000€*	*1. Trimestre*	*3. Terminé*
Alimentation secourue	*Directeur adjoint*	*1. Faible*	*2. Moins de 1000€*	*1. Trimestre*	*3. Terminé*
Contrat de maintenance informatique (intervention sous 4h)	*Directeur adjoint*	*1. Faible*	*2. Moins de 1000€*	*1. Trimestre*	*3. Terminé*
Accord sur le niveau de service de l'hébergeur	*Directeur adjoint*	*1. Faible*	*2. Moins de 1000€*	*1. Trimestre*	*3. Terminé*
Assurance multirisque professionnelle et sur les matériels informatiques	*Directeur*	*1. Faible*	*3. Plus de 1000€*	*1. Trimestre*	*3. Terminé*
Élaboration d'une politique de sécurité de l'information	*Directeur adjoint*	*2. Moyenne*	*1. Nul*	*1. Trimestre*	*2. En cours*
Rangement systématique des documents liés aux plans et calculs de structures dans un meuble fermé à clef	*Bureau d'études*	*1. Faible*	*1. Nul*	*1. Trimestre*	*1. Non démarré*
Chiffrement des fichiers liés aux plans et calculs de structures à l'aide de certificats électroniques	*Bureau d'études*	*2. Moyenne*	*1. Nul*	*1. Trimestre*	*1. Non démarré*
Création d'empreintes des fichiers liés aux plans et aux calculs de structure	*Bureau d'études*	*2. Moyenne*	*1. Nul*	*1. Trimestre*	*1. Non démarré*
Création d'empreintes des fichiers liés aux visualisations	*Bureau d'études*	*2. Moyenne*	*1. Nul*	*1. Trimestre*	*1. Non démarré*
…	*…*	*…*	*…*	*…*	*…*
Installation d'un antivirus sur les serveurs	*Directeur adjoint*	*1. Faible*	*2. Moins de 1000€*	*1. Trimestre*	*1. Non démarré*
Utilisation d'antivols pour les ordinateurs portables	*Service commercial*	*1. Faible*	*2. Moins de 1000€*	*1. Trimestre*	*1. Non démarré*
Utilisation de films empêchant l'espionnage de l'écran des ordinateurs portables	*Service commercial*	*1. Faible*	*2. Moins de 1000€*	*1. Trimestre*	*1. Non démarré*
Destruction des documents sensibles lors de leur mise au rebut	*Tous*	*1. Faible*	*2. Moins de 1000€*	*1. Trimestre*	*1. Non démarré*
Pose de barreaux aux fenêtres	*Directeur adjoint*	*1. Faible*	*3. Plus de 1000€*	*1. Trimestre*	*1. Non démarré*
Mesures de l'année					
Établissement de la liste des exigences réglementaires	*Directeur adjoint*	*1. Faible*	*1. Nul*	*2. Année*	*1. Non démarré*
Test trimestriel des fichiers sauvegardés	*Directeur adjoint*	*2. Moyenne*	*1. Nul*	*2. Année*	*1. Non démarré*
Vérification des empreintes des fichiers liés aux devis de manière régulière	*Directeur adjoint*	*2. Moyenne*	*1. Nul*	*2. Année*	*1. Non démarré*
…	*…*	*…*	*…*	*…*	*…*
Marquage du besoin de confidentialité des documents électroniques liés aux devis	*Service commercial*	*2. Moyenne*	*1. Nul*	*2. Année*	*1. Non démarré*
Marquage du besoin de confidentialité des documents papiers liés aux devis	*Service commercial*	*2. Moyenne*	*1. Nul*	*2. Année*	*1. Non démarré*
Extension de l'assurance aux risques d'altération d'informations	*Directeur*	*2. Moyenne*	*2. Moins de 1000€*	*2. Année*	*1. Non démarré*

Extension de l'assurance aux risques de vol d'informations	*Directeur*	*2. Moyenne*	*2. Moins de 1000€*	*2. Année*	*1. Non démarré*
Utilisation de scellés sur les ordinateurs afin de pouvoir constater leur ouverture non désirée	*Directeur adjoint*	*1. Faible*	*2. Moins de 1000€*	*2. Année*	*1. Non démarré*
Formation des personnels aux outils métiers et aux mesures de sécurité	*Directeur adjoint*	*2. Moyenne*	*3. Plus de 1000€*	*2. Année*	*1. Non démarré*
Mesures dans les trois ans					
Gestion des vulnérabilités sur les serveurs	*Directeur adjoint*	*3. Élevée*	*1. Nul*	*3. 3 ans*	*1. Non démarré*
Gestion des vulnérabilités sur Windows XP	*Directeur adjoint*	*3. Élevée*	*1. Nul*	*3. 3 ans*	*1. Non démarré*
Gestion des vulnérabilités sur MacOS X	*Directeur adjoint*	*3. Élevée*	*1. Nul*	*3. 3 ans*	*1. Non démarré*
Établissement d'un accord d'échange d'informations avec les clients et les partenaires	*Directeur adjoint et partenaires*	*2. Moyenne*	*1. Nul*	*3. 3 ans*	*1. Non démarré*
Mise en place d'un système RAID logiciel	*Directeur adjoint*	*3. Élevée*	*3. Plus de 1000€*	*3. 3 ans*	*1. Non démarré*

Exemple d'action type 5.2.2. Analyser les risques résiduels

Exemple

Un ensemble de risques subsiste après la mise en œuvre des mesures de sécurité formalisées :

Risque lié à l'altération d'un devis qui doit rester rigoureusement intègre

Niveau de risque				
Gravité	*1. Négligeable*	*2. Limitée*	***3. Importante***	*4. Critique*
Vraisemblance	***1. Minime***	~~*2. Significative*~~	~~*3. Forte*~~	*4. Maximale*

Risque lié à la compromission d'un devis au-delà du personnel et des partenaires

Niveau de risque				
Gravité	*1. Négligeable*	***2. Limitée***	~~*3. Importante*~~	*4. Critique*
Vraisemblance	*1. Minime*	***2. Significative***	~~*3. Forte*~~	~~*4. Maximale*~~

Risque lié à l'altération de plans ou de calculs de structures qui doivent rester rigoureusement intègres

Niveau de risque				
Gravité	*1. Négligeable*	*2. Limitée*	***3. Importante***	~~*4. Critique*~~
Vraisemblance	***1. Minime***	~~*2. Significative*~~	*3. Forte*	*4. Maximale*

Risque lié à la compromission de plans ou calculs de structures au-delà des personnels et partenaires

Niveau de risque				
Gravité	*1. Négligeable*	***2. Limitée***	~~*3. Importante*~~	*4. Critique*
Vraisemblance	*1. Minime*	***2. Significative***	~~*3. Forte*~~	~~*4. Maximale*~~

Exemple d’action type 5.2.3. Prononcer l'homologation de sécurité

Exemple

Le Directeur d'@RCHIMED a prononcé l'homologation de sécurité du cabinet au vu de l'étude réalisée (délimitation du périmètre, appréciation des risques, élaboration du plan d'action, mise en évidence des risques résiduels…) et des livrables élaborés (note de cadrage, note de stratégie, politique de sécurité de l'information).

Cette homologation de sécurité est valable un an et pourra être renouvelée tous les ans.

La mise en œuvre du plan d'action devra être démontrée, ainsi que l'amélioration continue de l'étude de sécurité.