POLITIQUE DE SECURITE DE L'INFORMATION

thinkproject

ISMS

Système de Management : ISMS
Produits : TOUS
ID du Document : ISMS_00001
Version : 1.0
Classification : Ouverte

Créé par	Andreas Blücher	13.07.2021
Approuvé par	Tom Harman	13.07.2021
Date d'émission originale	29.04.2020	

Veuillez ne pas imprimer de copie de ce document.

TABLE DES MATIÈRES

1 OBECTIF

Le groupe Thinkproject est un collectif de solutions digitales et de professionnels leaders sur le marché dont l'objectif est de développer et de fournir les meilleures solutions pour soutenir, connecter et faire progresser l'industrie de la construction et les personnes qui la composent.

Cela inclut le traitement des informations et des données pour le compte de nos clients. Par conséquent, les informations des clients doivent être protégées en termes de confidentialité, d'intégrité et de disponibilité. La présente politique de sécurité de l'information décrit comment atteindre cet objectif. La sécurité de l'information est établie au moyen d'un système de gestion de la sécurité de l'information (*ISMS*) conforme à la norme ISO 27001. Il s'agit d'une norme industrielle pour la sécurité de l'information. Le *ISMS* fournit des politiques, des processus et des concepts pour assurer la sécurité de l'information.

Au sein du groupe Thinkproject, tous les processus importants relatifs à la sécurité de l'information sont centralisés. Ces processus centralisés garantissent des normes de sécurité de l'information à l'échelle du groupe. Chaque filiale travaille au même niveau de sécurité de l'information avec ces processus centralisés. Il existe des processus centralisés pour la gestion des actifs, la gestion des risques et les incidents de sécurité de l'information.

En plus des processus centralisés, il existe des processus locaux pour les techniques ou outils spécifiques utilisés dans les filiales.

1.1 Publication

Le Président Directeur Général (PDG) de Thinkproject a publié cette politique de sécurité de l'information après en avoir fait l'examen. Tous les employés sont instruits d'appliquer ces règles. Il est également demandé à tous les employés de se comporter de manière responsable et de tenir compte de la sécurité de l'information de manière efficace et dans le respect de la loi.

1.2 Contrôles et sanctions

La politique de sécurité de l'information est obligatoire pour tous ceux qui, dans leur champ d'application, travaillent pour ou avec les filiales du groupe Thinkproject. Cela inclut les employés, les consultants, les prestataires de services et les fournisseurs. La conformité à l'ISMS sera examinée régulièrement et au cas par cas. Chaque employé des filiales de Thinkproject doit respecter la politique de sécurité de l'information et toutes les normes et lignes directrices qui en découlent. Les violations de ses directives seront poursuivies et des mesures disciplinaires seront prises.

1.3 Point de contact

Les demandes de renseignements, les suggestions et les critiques sont toujours les bienvenues. Veuillez les adresser, ainsi que toute plainte, au responsable de la sécurité de l'information de Thinkproject.

Munich, Avril 2021

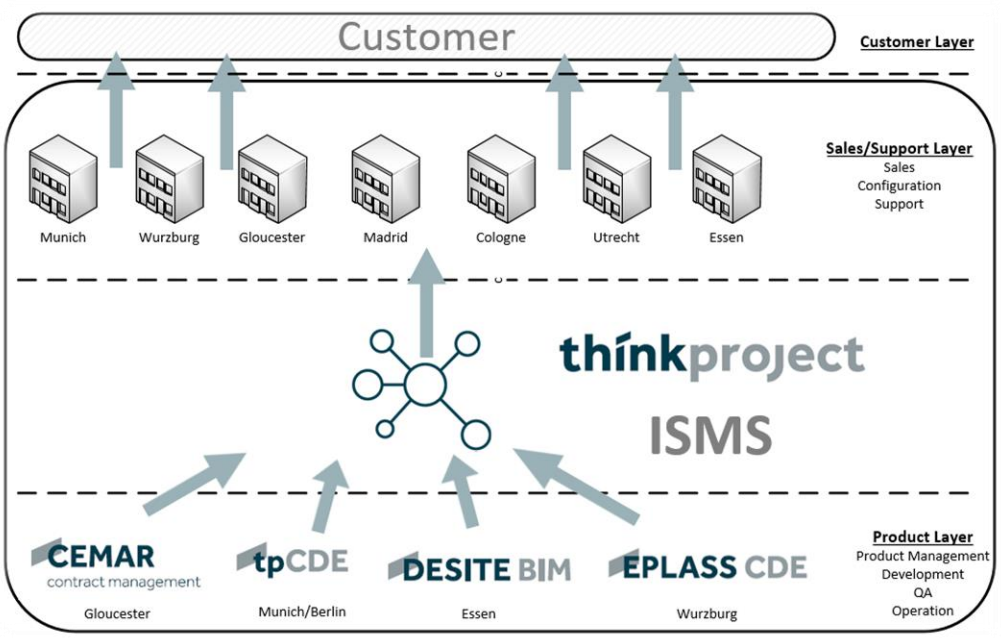
Patrik Heider, PDG

2 PÉRIMÈTRE

La portée d'un *ISMS* décrit ce qui doit être considéré du point de vue de la sécurité de l'information et ce qui ne le sera pas. Le champ d'application de *l'ISMS* de Thinkproject couvre les éléments suivants :

Localisations

- Munich
- Gloucester
- Wurzburg
- Berlin
- Cologne
- Madrid
- Essen
- Utrecht



Produits

- Thinkproject CDE
- EPLASS CDE
- CEMAR
- DESITE

Services

- Gestion des produits
- Développement de logiciels, y compris les tests
- Exploitation du logiciel, y compris l'hébergement
- Ventes
- Configuration du logiciel
- Support client

- Informatique interne du bureau
- Gestion des utilisateurs
- Administration

Ces services comprennent des activités de ventes et de support.

Bien qu'il y ait des produits et des filiales du groupe Thinkproject qui ne sont pas dans le champ d'application, ils doivent appliquer les normes *ISMS* dès qu'il est possible. Cela pourrait être nécessaire pour atteindre un niveau de sécurité des informations qui pourrait être exigé par le GDPR.

2.1 Champs d'Application de l'*ISMS* dans les Certificats

La conformité de l'*ISMS* de Thinkproject à la norme ISO 27001 est vérifiée chaque année par un organisme de certification externe. Le résultat de ce contrôle est un certificat qui peut être remis aux clients pour démontrer la conformité à la norme ISO 27001.

Ce certificat contient un champ d'application qui est présenté ici dans un souci d'exhaustivité :

Les fonctions de l'entreprise qui sont impliquées dans la création et l'exploitation de la plateforme d'intelligence constructive Thinkproject (tpCDE, EPLASS CDE, CEMAR, DESITE BIM). Cela concerne les opérations, les services professionnels, la gestion des produits, le développement des produits, la gestion de la qualité, le marketing, l'administration et les finances.

3 DÉFINITIONS ET ABRÉVIATIONS

3.1 Sécurité de l'Information

La sécurité de l'information couvre les propriétés des systèmes de traitement de l'information et des unités organisationnelles qui garantissent la confidentialité, l'intégrité et la disponibilité des informations. La sécurité de l'information sert à protéger contre les dangers et les menaces, à prévenir les dommages et à minimiser les risques.

3.2 ISMS

Un système de gestion de la sécurité de l'information (*ISMS*) est considéré comme la composante d'un système de gestion à l'échelle du groupe qui couvre l'établissement, la mise en œuvre, l'exécution, l'évaluation, la maintenance et l'amélioration de la sécurité de l'information sur la base d'une approche des risques commerciaux. Le *ISMS* couvre les structures, les directives, les activités de planification, les responsabilités, les pratiques, les méthodes, les processus et les ressources du groupe.

Le groupe Thinkproject dispose d'un ISMS conforme à la norme ISO 27001.

4 OBJECTIFS ET PRINCIPES

4.1 Objectifs

Les objectifs de sécurité de l'information des sociétés thinkproject sont les suivants :

- La **satisfaction des exigences des clients** en matière de confidentialité, d'intégrité et de disponibilité.
- Le **soutien fiable** des processus d'entreprise par l'utilisation des technologies de l'information et par la garantie de la continuité des flux de travail au sein de l'organisation.
- La réalisation de **communications plus sûres et plus fiables** avec les clients, les autorités et les fournisseurs de services externes.
- La **préservation de la valeur** investie dans la technologie, l'information, les processus de travail et les connaissances.
- La sécurisation de la **valeur élevée de l'information.**
- Le **respect des exigences** résultant des directives légales.
- La garantie du droit à l'autodétermination informationnelle des parties concernées par le traitement des informations personnelles (**protection des données**).
- La **réduction des coûts** résultant d'incidents.

4.2 Principes

Lors de la création de lignes de base et de concepts de sécurité de l'information, les principes suivants doivent être pris en compte :

4.2.1 Adéquation

Des mesures sont prises afin d'atteindre un niveau plus élevé de sécurité de l'information. Ces mesures impliquent des coûts. Le principe d'adéquation garantit qu'il existe un rapport raisonnable entre l'augmentation des coûts et l'augmentation du niveau de sécurité de l'information.

4.2.2 Ressources

Des ressources financières, humaines et temporelles suffisantes sont mises à disposition afin d'atteindre et de maintenir un niveau approprié de sécurité des informations.

4.2.3 Implication des employés

La sécurité de l'information concerne tous les employés. Chacun doit contribuer à prévenir les dommages par une conduite responsable et une sensibilisation à la sécurité.

4.2.4 Classification des informations

Toutes les informations traitées dans le cadre des processus d'entreprise sont classées en fonction de leurs besoins de protection. Il s'agit d'une condition préalable à l'évaluation des risques et à la mise en œuvre de contrôles de sécurité appropriés. Les informations sont classées selon les catégories de protection que sont la confidentialité, l'intégrité et la disponibilité.

5 RESPONSABILITÉS

Les rôles/responsabilités suivants assurent le bon fonctionnement de notre système de gestion de la sécurité de l'information :

5.1 Responsabilité Personnelle

Dans le cadre de l'exercice de ses fonctions, chaque employé est responsable des informations, des processus et des flux de travail qui lui sont confiés. Il incombe à chaque employé de maintenir un niveau élevé de sécurité de l'information. Une chaîne est aussi forte que son maillon le plus faible. L'organisation interne de la sécurité de l'entreprise est clairement structurée afin de soutenir cette démarche.

5.2 Conseil d'Administration de l'ISMS

Le conseil de l'*ISMS* gère tous les processus centralisés de l'*ISMS*, comme la gestion des actifs, des risques et des contrôles. Le conseil est responsable de l'orientation stratégique et de l'amélioration de l'*ISMS*. Le conseil se réunit régulièrement et rend compte à l'équipe de direction.

5.3 Propriétaire du Processus

Chaque processus qui concerne la sécurité de l'information a un propriétaire. Celui-ci est responsable de la définition du processus et de son application. Les descriptions de processus garantissent que chaque employé est sur la même longueur d'onde.

5.4 Propriétaire de l'Actif

Du point de vue de la sécurité de l'information, un actif est tout ce qui est lié à l'information ou au traitement de l'information. Il peut s'agir d'un ordinateur, d'une base de données, d'un système de stockage ou d'un logiciel, par exemple. Les actifs jouent un rôle important dans la sécurité de l'information. C'est pourquoi chaque actif est attribué à un propriétaire qui est responsable de cet actif. Les actifs sont conservés dans un registre des actifs.

5.5 Propriétaire du Risque

Les actifs sont menacés par des risques. Des mesures sont prises afin de réduire l'impact des risques ou leur probabilité d'occurrence. Chaque risque est attribué à un propriétaire du risque. Dans la plupart des cas, le propriétaire du risque est la même personne que le propriétaire de l'actif menacé.

5.6 Management Supérieur

La direction générale fournit toutes les ressources nécessaires au bon fonctionnement de l'*ISMS*. Il est important que la direction générale s'engage envers le *ISMS*. Lors de la revue de direction, le responsable de la sécurité de l'information du groupe rend compte de son état actuel.

En outre, la direction générale est responsable de l'amélioration continue de l'*ISMS*. Cela se fait en suivant le modèle PDCA.

5.7 Responsable de la Sécurité de l'Information du Groupe

En collaboration avec le Conseil de l'*ISMS*, le responsable de la sécurité de l'information du groupe dirige tous les processus centralisés de l'*ISMS*.

- Revue de direction
- Modération du Conseil de l'*ISMS*
- Gestion du SoA
- Définition des normes
- Gèrance des programmes d'audit externe et interne

Le responsable de la sécurité de l'information du groupe est chargé de veiller à ce que le *ISMS* du groupe soit prêt pour la certification. Il doit notamment s'assurer que tous les produits et sites satisfont aux contrôles pertinents de la norme ISO 27001.

5.8 Responsable Local de la Sécurité de l'Information

Chaque site du périmètre désigne une personne responsable de la mise en œuvre locale de l'*ISMS*. Cela comprend les tâches suivantes :

- Participer régulièrement au conseil d'administration de l'ISMS
- Gérer les actifs locaux dans le registre centralisé des actifs
- Identifier les risques locaux
- Préparer le site pour les audits internes et externes

- Participer aux réunions du conseil d'administration de l'ISMS
- Réaliser des formations de sensibilisation
- Suivi des processus locaux

5.9 Délégué à la Protection des Données

Les conditions dans lesquelles les entreprises sont tenues de désigner un délégué à la protection des données sont régies par la législation nationale. Il est conseillé aux entreprises de demander conseil sur cette question à un avocat spécialisé dans le droit de la protection des données.

Néanmoins, chaque site relevant du champ d'application désigne une personne responsable de la protection des données sur place. Cette responsabilité comprend :

- S'assurer que les processus et les produits sont conformes au GDPR et aux réglementations spécifiques du pays.
- La tenue des registres locaux des activités de traitement (article 30 du GDPR).
- Les interactions avec les autorités de protection des données.
- Les interactions avec les clients pour les questions de protection des données.

6 PROCESSUS DE SECURITE DE L'INFORMATION ET GESTION DES RISQUES

Les exigences de protection sont basées sur les informations à protéger. L'exigence de protection est ensuite transférée aux processus, aux applications informatiques, aux bases de données, aux serveurs, aux ordinateurs personnels, aux réseaux, aux locaux, etc. ainsi qu'aux bâtiments et aux terrains si nécessaire.

L'exigence de protection est justifiée par les catégories de protection suivantes :

- Confidentialité
- Intégrité
- Disponibilité

Différents niveaux de protection sont définis au sein de chaque catégorie de protection.

6.1 Confidentialité

La confidentialité est la caractéristique d'un élément d'information qui n'est destiné qu'à un groupe limité de destinataires (personnes, unités, processus). L'information est protégée contre toute consultation non autorisée et ne doit pas être révélée sans l'autorisation du propriétaire de l'information.

Tableau 1 : Niveau de protection de la confidentialité

Niveau de Protection	Description
Ouvert	Aucune confidentialité prescrite.
Restreint	Une violation de la confidentialité est considérée comme un risque normal lorsque l'impact attendu est faible ou nul.
Confidentiel	Une violation de la confidentialité pourrait entraîner un impact commercial important (y compris une perte financière limitée) ou avoir un impact négatif sur une personne ou un groupe.
Sensible	Une violation de la confidentialité entraînerait un risque grave pour les activités de l'entreprise (y compris une perte financière importante) ou mettrait en danger une personne ou un groupe.

Une mesure permettant d'atteindre une plus grande confidentialité pourrait être, par exemple, le cryptage.

6.2 Integrité

L'intégrité désigne le caractère approprié (intact) et complet des informations et le bon fonctionnement des systèmes. Les informations doivent être protégées contre la falsification et la perte.

Tableau 2 : Niveau de protection de l'intégrité

Niveau de Protection	Description
Normal	Une perte d'intégrité est considérée comme un risque normal lorsque l'impact attendu est faible ou nul.

Moyen	Une perte d'intégrité est considérée comme un risque grave lorsqu'un impact significatif peut en résulter. Un effet négatif sur l'intégrité personnelle ne peut être exclu.
Elevé	Une perte d'intégrité entraînerait un risque extrême pour les activités de l'entreprise (y compris des pertes financières importantes ou la ruine de la société) ou mettrait une personne ou un groupe en danger.

6.3 Disponiblité

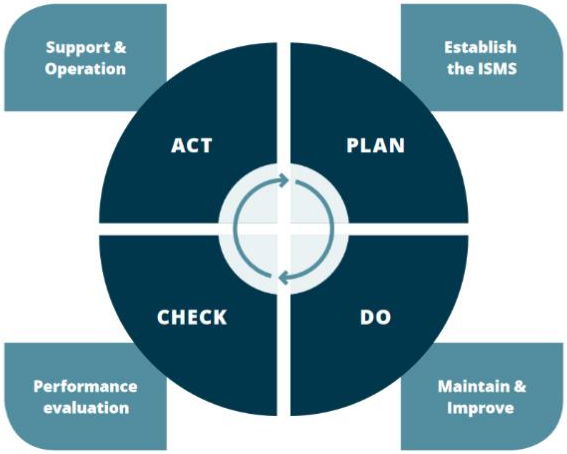
La disponibilité est une mesure de la période pendant laquelle un élément d'information (un système) est disponible pour les processus d'affaires. Cette catégorie de protection est définie comme une période de temps d'arrêt tolérable pour chaque période de temps désignée.

Tableau 3 : Niveau de protection pour la disponibilité

Niveau de Protection	Description
Normal	Les défaillances du système et les pertes de disponibilité des informations sont évaluées comme des risques normaux lorsque l'impact attendu est faible ou nul.
Moyen	Les pannes de système et les pertes de disponibilité des informations sont considérées comme des risques graves lorsqu'elles peuvent avoir un impact significatif, ou lorsque l'image publique de l'entreprise ou les relations avec les clients peuvent être endommagées.
Elevé	Les défaillances du système et les pertes de disponibilité des informations sont considérées comme des risques extrêmement graves qui pourraient entraîner la ruine de la société ou de l'économie, porter durablement atteinte à l'image de marque de l'entreprise ou détériorer définitivement les relations avec les grands comptes.

6.4 Modèle PDCA

Le processus de sécurité de l'information à l'échelle de l'entreprise permet de garantir les objectifs et la qualité de l'*ISMS* grâce à un modèle contenant les phases Plan, Do, Check and Act (modèle PDCA selon ISO 9001).



6.5 Planification de l'ISMS (Plan)

L'*ISMS* est planifié selon un modèle PDCA sous les auspices du responsable de la sécurité de l'information. Les informations et les éléments de sécurité sont identifiés et documentés sur la base d'une détermination de la sensibilité.
Les concepts et directives de sécurité sont créés à la base de la politique de sécurité de l'information (y compris, par exemple, le concept de protection des données, le concept de protection contre les virus, le concept de mesures d'urgence et les règlements relatifs à l'utilisation des systèmes informatiques).

6.6 Soutien et exploitation de l'*ISMS* (Do)

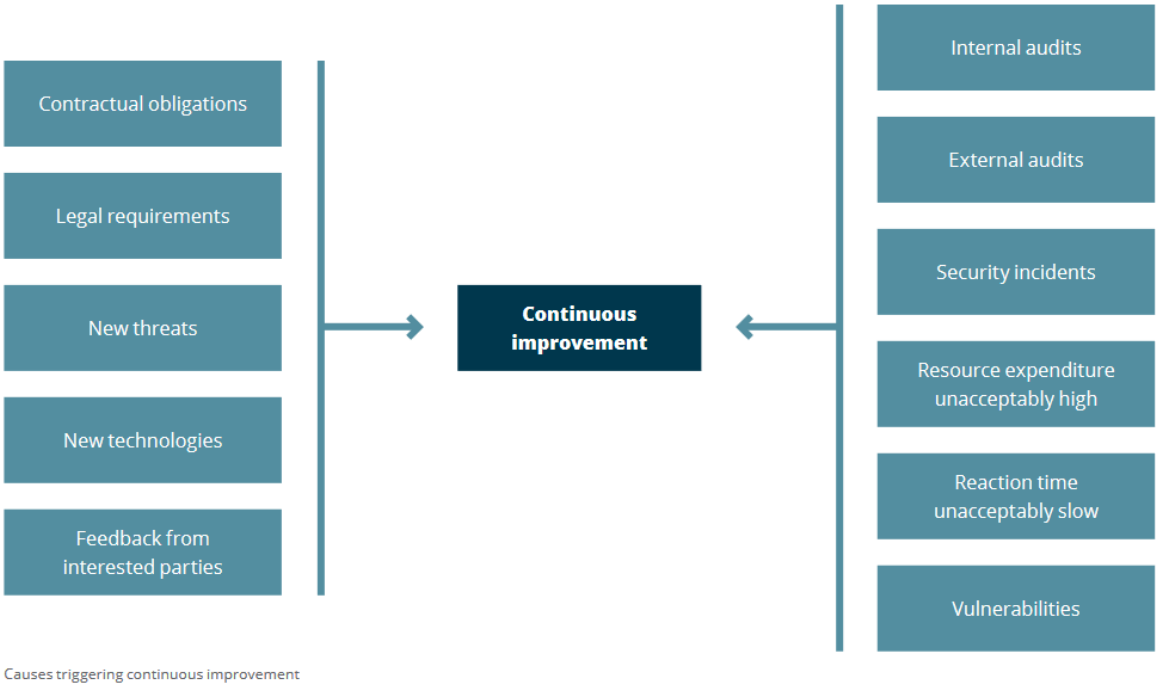
Les règles et mesures organisationnelles et techniques définies dans la phase de planification doivent ensuite être mises en œuvre et documentées. Les résultats obtenus en dehors de l'exploitation sont documentés sous forme de journaux ou d'autres enregistrements et sont mis à disposition pour des analyses, des corrections d'erreurs et des améliorations.

6.7 Suivi de l'*ISMS* (Check)

Tous les employés sont tenus de signaler les incidents de sécurité à leurs supérieurs ou directement au responsable de la sécurité de l'information. Il peut s'agir, par exemple, d'alertes virales, de tentatives d'accès non autorisées avérées, de la perte de dispositifs de stockage numérique mobiles, d'une disponibilité insuffisante des informations ou d'une représentation incorrecte des informations. Le responsable de la sécurité de l'information classe les incidents signalés et met en œuvre des contrôles supplémentaires. L'efficacité de l'*ISMS* est vérifiée chaque année par le responsable de la sécurité de l'information au moyen d'audits internes. En outre, un audit annuel sera effectué par un organisme de certification externe.

6.8 Amélioration de l'ISMS (Act)

Les non-conformités et recommandations constatées lors des audits internes et externes seront constamment et rapidement vérifiées et mises en œuvre par des mesures appropriées. L'efficacité et la qualité de l'*ISMS* seront évaluées à l'aide d'indicateurs clés de performance.

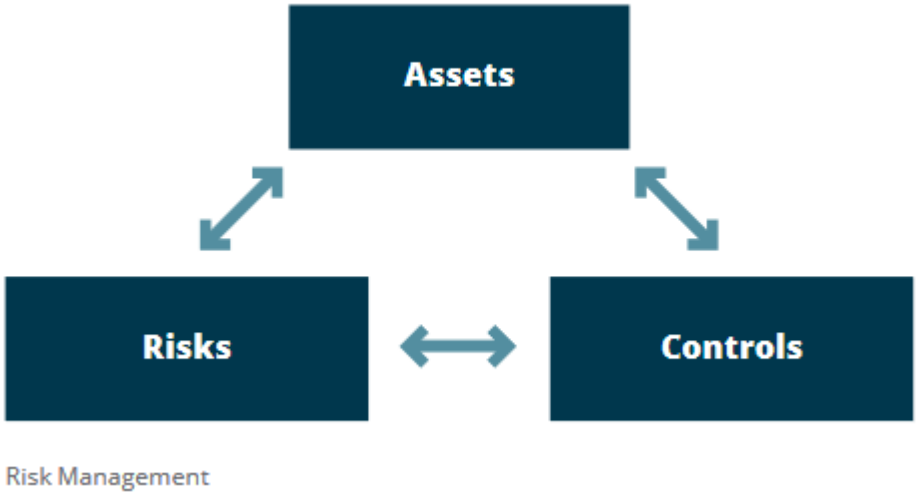


Causes triggering continuous improvement

L'amélioration continue se concentre sur les actions préventives et sur les contrôles qui ont le plus grand effet tout en utilisant le moins de ressources possible.

6.9 Evaluation du Risque

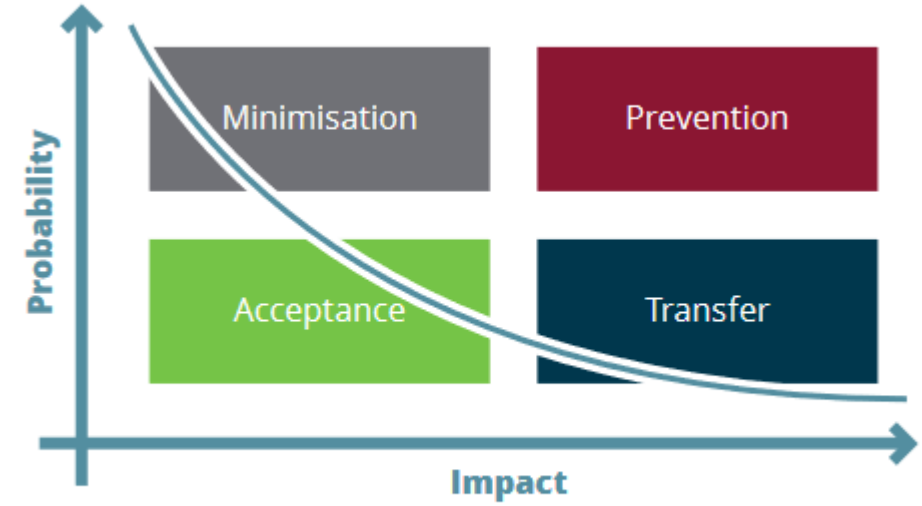
Les analyses de risques sont un élément important de l'*ISMS*. Elles sont utilisées pour identifier et évaluer les risques. Par le biais d'actions préventives, elles sont également utilisées pour empêcher, minimiser ou transférer des événements négatifs à des tiers. En outre, ils sont utilisés pour communiquer sur des situations de risques, par exemple, afin de promouvoir la perception d'un risque. Sur la base des actifs identifiés possédant une exigence de protection attribuée, des scénarios sont envisagés dans lesquels des vulnérabilités aux menaces potentielles apparaîtront. Après avoir évalué la probabilité d'occurrence d'une menace et le niveau d'impact qui en résulte, les contrôles respectifs doivent être déterminés de manière technique et organisationnelle. Ceux-ci doivent ensuite être évalués en fonction de leurs coûts de mise en œuvre, du temps nécessaire pour les mettre en œuvre et de leur efficacité.



Risk Management

Les actifs sont menacés par des risques. Des mesures et des contrôles sont pris pour atténuer l'occurrence des risques.

Dans des cas justifiés, au lieu de prévenir, de minimiser ou de transférer le risque, il peut être décidé de le prendre activement en charge, pour autant que cela n'enfreigne aucune loi, aucun règlement ni aucun contrat. L'acceptation de tels risques est réservée à la décision de la direction générale.



Handling of risks

Les risques sont calculés comme le produit de l'impact et de la probabilité. Le graphique ci-dessus montre une ligne de risque constant. En outre, quatre étapes de traitement du risque sont indiquées. Veuillez vous référer au processus de risque de Thinkproject pour plus d'informations détaillées.

7 NORMES ET RÈGLES DE SÉCURITÉ

Outre notre système de gestion de la sécurité des systèmes d'information (*ISMS*) basé sur la norme ISO27001, la législation sur la protection des données (GDPR) doit être prise en compte dans le cadre de la sécurité des informations. La protection des données se concentre davantage sur la confidentialité et l'intégrité que sur la disponibilité. Du point de vue d'un éditeur de logiciels, les principes "Privacy by Design" et "Privacy by Default" jouent un rôle important.

8 CONTRÔLE DES DOCUMENTS

Version	Date	Auteur	Approuvé par	Details des modifications apportées
1.0	14.02.2020	AB	Peter Mezger	Première version
1.2	19.02.2020	TH	Peter Mezger	Feedback Tom, prêt à être distribué au conseil d'administration de l'ISMS
1.4	17.03.2020	AB	Peter Mezger	Feedback au conseil de l'ISMS Board, nouveau modèle
1.6	18.03.2020	AB	Jules van der Weide	Ajout de la ville d'Utrecht dans le chapitre 2
1.8	29.04.2020	RG	Gareth Burton	Communiqué par le PDG et le directeur financier
2.0	02.09.2020	AB	AB	Feedback Alan Brooks (DPO, définition des niveaux de protection)
2.2	26.11.2020	AB	Gareth Burton	Feedback de l'organisme de certification (Engagement Top Management PDCA, périmètre officiel du certificat)
2.4	19.04.2021	AB	Patrik Heider	Communiqué par le nouveau PDG
1.0	13.07.2021	AB	TH	Nouvelle numérotation des versions en raison de l'importation dans OneTrust