

Dominik Spiess

Qui profite de l'approche d'audit orientée risques?

Propositions concrètes pour un contrôle des risques amélioré

Il est incontestable que l'approche d'audit orientée risques s'impose de plus en plus dans les entreprises. Les divers articles publiés dans le présent numéro en témoignent. L'auteur aimerait maintenant examiner la question de savoir qui en profite en dernier lieu. S'agit-il seulement de l'intérêt personnel propre au réviseur lui permettant d'exécuter ses travaux dans de meilleures conditions, de manière plus efficace et en réduisant le risque d'audit? Dans quelle mesure le client peut-il également en tirer profit? Quelle est l'importance de la gestion des risques dans les entreprises? Quel est à cet égard le rôle du conseil d'administration? Last but not least, l'auteur donne quelques rappels pratiques en matière de gestion des risques.

1. Définition du risque

Le risque d'entreprise est «la vraisemblance qu'un événement influence négativement la capacité d'une organisation d'atteindre avec succès ses objectifs et ses stratégies d'entreprise» [1]. Exception faite des organisations à but non lucratif, la réalisation de bénéfices est l'un des principaux objectifs de la plupart des entreprises. Le risque d'entreprise est dès lors étroitement lié à la variabilité du bénéfice.

On relèvera en premier lieu que le bénéfice ou la perspective d'un bénéfice ne constitue pas seulement une grandeur souhaitable mais qu'il revêt également une importance micro et macro-économique. Au niveau de l'entreprise, ils sont nécessaires pour réunir le capital-actions ou «capital risque», qui finance la société au moment de son

démarrage et lors de son expansion (comportant des risques), pour maintenir le capital et la valeur de l'entreprise



Dominik Spiess, lic. HEC, expert-comptable diplômé, membre de la Commission d'audit de la Chambre fiduciaire, Dominik Spiess SA, Genève

et pour rémunérer le capital par la distribution de dividendes. La réalisation de cash flow libre («free cash flow») permet de procéder à des investissements supplémentaires, de réduire l'endettement, de distribuer des bonis aux collaborateurs, d'augmenter les salaires, etc.

Les analystes financiers font découler la valeur d'une entreprise dans une large mesure de sa capacité à réaliser du cash flow libre et du bénéfice. Ce critère a été ces derniers temps relégué au second plan en ce sens que de nombreuses start-ups sont analysées sur la base d'autres éléments tels que la capacité d'innovation, l'âge moyen des collaborateurs, leur formation, le chiffre d'affaires, voire le «burn-rate», c'est-à-dire le contraire du bénéfice. Même au-delà de ces considérations, l'aspect bénéfice reste finalement pertinent car les facteurs précités doivent de nouveau, si on les considère à long terme, refléter la capacité de l'entreprise de réaliser des bénéfices.

Le risque inhérent d'une entreprise correspond dans son ensemble à la probabilité selon laquelle ses résultats se développent de manière imprévisible. Cette évolution peut être aussi bien positive que négative. Si ses résultats varient subitement de -50% ou de +100%, une entreprise est considérée comme étant à risque, à moins que cette évolution n'ait été prévisible. Ce phénomène peut être observé souvent dans les banques qui présentent parfois des résultats en forte fluctuation. La cause en réside souvent dans les résultats de négoce. Les opérations de trading dans les banques (devises, titres, instruments financiers dérivés, matières premières, etc.) sont soumises aux fluctuations de cours parfois importantes des marchés concernés. Souvent, la constitution de

corrections de valeur sur les risques de crédit encourus par la banque influence aussi les résultats de manière imprévue. Le dernier exemple en date est celui de la Banque Cantonale de Genève. Les risques de crédit et de marché sont toutefois contractés par exemple par l'UBS «de manière consciente et active, comme partie intégrante des prestations de service» [2].

La plupart des entreprises, qu'elles soient cotées en bourse ou qu'il s'agisse de PME, essaient de réduire ce caractère imprévisible et de donner l'image de sociétés qui ne cessent de s'améliorer. L'évolution des résultats doit être aussi régulière que possible ou au moins suivre une règle constante. La comptabilité et les principes d'établissement des comptes jouent également un rôle essentiel dans ce contexte, ce dont tient compte aussi le réviseur dans sa stratégie d'audit [3].

Les efforts faits pour se présenter en tant qu'entreprise à risque réduit résultent du fait qu'un risque accru est lié à des coûts accrus, par exemple dans le rating de crédit des banques. Mais ce qui est encore plus important, c'est qu'en règle générale les stakeholders (actionnaires, créanciers, collaborateurs, Etat, population locale) ont tout intérêt à avoir une entreprise solide. Telle est même souvent la condition pour entrer en relations commerciales.

Cette situation devrait mener presque obligatoirement à la mise en place d'une gestion intégrée des risques. Or, il n'en est souvent pas ainsi dans la pratique.

2. Développement et importance des risques

On peut distinguer deux catégories de risques d'affaires: en premier lieu, les *risques directs* qui sont sciemment pris et à l'aide desquels l'entreprise réalise son bénéfice. Il s'agit des risques qui renferment régulièrement aussi une opportunité: par exemple, une banque conclut en toute connaissance de cause des risques de crédit pour réaliser ainsi un bénéfice par une marge d'intérêt. En second lieu, les *risques indirects*. Il s'agit là des risques qui exercent au se-

cond plan une influence sur l'entreprise et qui ne sont pas en rapport direct avec ses activités-clés (p. ex. marketing, environnement, personnel, relations publiques) [4]. Ce qui est important dans cette distinction, c'est que ces derniers risques sont généralement mal appréhendés et par conséquent moins bien contrôlés.

Il est évident que les risques ne cessent de se modifier et que de nouveaux risques apparaissent en permanence. Ce qui est relativement nouveau, cependant, c'est le rythme des changements et, partant, celui du potentiel de chances/dangers. La globalisation du monde des affaires, également liée à l'évolution de l'Internet, signifie aujourd'hui par exemple que, dans le secteur tertiaire, un nouveau concurrent peut entrer en jeu en l'espace de quelques mois, concurrent pouvant éventuellement opérer à des milliers de kilomètres de distance. Cette situation fait en sorte que d'inimaginables possibilités d'activité s'offrent aux entreprises «ouvertes», c'est-à-dire à celles qui utilisent les nouvelles possibilités de l'Internet. Leurs concurrents sont dès lors exposés de la même manière à une menace intensive pesant sur les marchés de l'écoulement.

Cette accélération de la vie des affaires a aujourd'hui aussi pour conséquence par exemple qu'un manager peut être amené à absorber 100 à 200 messages e-mail par jour. L'opportunité consiste pour lui à pouvoir agir plus vite et plus globalement. Un risque nouveau dans ces circonstances vient de ce que ce manager n'arrive peut-être plus à déceler l'essentiel parmi la multitude des messages qu'il reçoit. Cet exemple entend également montrer qu'une telle situation n'existait pas il y a encore trois ans.

Des risques spécifiques et plus «nouveaux» pouvant exercer aujourd'hui une forte influence sur une entreprise sont les suivants:

- de nouvelles lois, par exemple concernant la responsabilité civile en matière de produits;
- l'influence de la politique qui court-circuite de fait certaines lois (cf. fonds en déshérence);

- l'évolution technologique, la réduction du cycle de vie des propres produits;
- les nouvelles pratiques commerciales comme l'application d'honoraires en fonction du résultat ou le recours accru aux actions en responsabilité;
- les risques de l'environnement;
- les risques menaçant la réputation, par exemple par diffamation ou par une crise mal surmontée;
- les risques dans le domaine du personnel, par exemple réactions négatives en cas de licenciement ou des systèmes de rémunération agressifs.

Du fait qu'une entreprise n'est pas exposée aux seuls risques directs mais également à des risques indirects sans en avoir véritablement l'intention et parce que ces risques peuvent se modifier rapidement, il peut en résulter un *effet de surprise* auquel on ne peut remédier qu'en appliquant une stratégie de risque complète. Cela signifie que le thème «risque» doit être abordé dans son intégralité et que tous les risques majeurs doivent être couverts.

3. Situation de la gestion des risques dans les entreprises

En dépit de cette affirmation à vrai dire lapidaire et des articles qui traitent abondamment du sujet, *la gestion des risques n'est pas intégralement résolue dans la plupart des entreprises*. Ce n'est pas seulement ce que l'auteur a constaté dans le cadre de son activité d'expert-comptable et de conseiller mais c'est là aussi un fait avéré [5]. Cette remarque n'a cependant pas de raison d'être la plupart du temps s'il s'agit d'un groupe ou d'une banque doté d'un service d'audit interne. En d'autres termes, on se trouvera pratiquement toujours face à une politique des risques globale dans les cas où l'entreprise dispose d'un service d'audit interne. Celui-ci implémente assez souvent le processus de surveillance des risques dans l'entreprise.

Les risques d'affaires directs, c'est-à-dire ceux qu'une entreprise est sciemment prête à affronter, sont le plus souvent bien contrôlés dans les entreprises rentables. L'audit interne qui soutient ce processus, dans les banques comme chez les négociants en valeurs mobilières et dans les groupes, fait aussi par-

tie des contrôles internes permettant de surveiller ces risques. Dans les établissements financiers, la gestion des risques est davantage organisée car elle se fonde sur une base légale, et dans le cas du trading et de l'utilisation de produits dérivés [6], sur une directive de l'Association suisse des banquiers.

Les risques indirects sont généralement appréhendés plus faiblement et mal contrôlés. Lorsqu'ils se réalisent, cela engendre souvent une réaction mal adaptée à la situation car on n'est justement pas préparé.

Pour cette raison, la *gestion de crise* est étroitement liée à la gestion des risques. Une crise survient en particulier lorsque le risque devient réalité, que l'entreprise y est mal préparée et qu'elle ne s'en préoccupe pas ou pas assez. La gestion de crise devrait être institutionnalisée dans toute grande entreprise comme cela est déjà le cas dans certains groupes. On veillera notamment à ce que l'entreprise et les activités opérationnelles ne soient pas paralysées par la crise. Dans les PME, un petit nombre de check-lists pourrait aider sensiblement à gérer les crises. Des règles cohérentes en matière de relations publiques sont en outre indispensables dans une situation de crise.

Un mécanisme de surveillance ne doit pas être mis en place pour chaque risque indirect décelable; ce serait trop coûteux. La politique globale des risques devrait en revanche comporter des principes couvrant également les risques indirects, ceux qui ne sont pas directement liés aux activités-clés de l'entreprise.

4. Rôle du conseil d'administration

La notion de «gestion des risques» n'existe pas dans le Code suisse des obligations. On ne la trouve pas non plus dans les index alphabétiques des spécialistes suisses en matière de Code des obligations que sont Böckli [7] et Forstmoser/Meier-Hayoz/Nobel [8]. Il n'existe actuellement pas de prescription explicite en Suisse sur ce thème. Comme le comprend l'auteur, la responsabilité de la gestion des risques ap-

partient en dernier lieu à la fonction de haute direction du conseil d'administration, en vertu de l'article 716a CO. Mais on ne peut pas en déduire, à l'inverse, qu'il pourrait en résulter une responsabilité en matière d'introduction d'un système de gestion des risques. Cependant, selon Böckli [9] il est «possible d'assimiler sans autre les connaissances des débats internationaux sur le corporate governance au droit suisse». Böckli est également d'avis que la gestion des risques peut être considérée comme l'une des notions-clés des débats sur le corporate governance, ce qui corrobore la thèse que la gestion des risques appartient par analogie à la haute direction du conseil d'administration. Le rôle de ce dernier se concentrera donc dans la plupart des cas sur l'approbation d'un cadre conceptuel et de directives, et il consistera à confier l'exécution de la gestion des risques à la direction. Celle-ci devrait être jugée pleinement responsable de l'interprétation, de l'adaptation régulière, de l'exécution et de la surveillance de la gestion des risques. C'est ce qui fait apparaître le caractère opérationnel marqué de la gestion des risques. Il ne serait dès lors pas correct de rechercher la responsabilité immédiatement au niveau du conseil d'administration en cas de défaillance d'un contrôle interne. De même, il serait faux de rattacher la responsabilité de la gestion des risques à l'audit interne, voire externe. La gestion des risques est une tâche de ligne et non une tâche d'état-major. Le management opérationnel est dès lors régulièrement considéré comme le service responsable de la gestion des risques.

Par exemple, le conseil d'administration de l'UBS est responsable de l'approbation des principes de gestion des risques et de contrôle, mais quant à la gestion des risques proprement dite, elle est du ressort de divers services de management [10].

La gestion des risques n'est pas évoquée dans l'avant-projet de Loi fédérale sur l'établissement et le contrôle des comptes annuels «LECCA». La seule précision apportée par la LECCA est l'obligation d'indiquer dans l'annexe aux comptes comment s'est exercée pendant l'exercice la surveillance

des risques découlant d'instruments financiers (art. 33 al. 3).

La situation est cependant autre dans les banques: la gestion des risques est une exigence légale car les banques doivent donner des explications sur ce point dans l'annexe aux comptes annuels. Rappelons l'existence des directives de l'Association suisse des banquiers sur ce point.

A l'étranger [11], l'évolution de ce thème est plus avancée. En Allemagne, le directoire doit veiller à l'existence d'un «système de surveillance approprié» comme le lui impose la KonTraG (Loi sur le contrôle et la transparence dans l'entreprise). Le London Stock Exchange exige, à partir de la fin de l'an 2000, que les sociétés cotées à cette bourse aient un système de contrôle interne approprié soumis à la surveillance du conseil d'administration. «The Board should maintain a sound system of internal control».

5. L'utilité de l'approche d'audit orientée risques pour l'entreprise auditée

Il ressort d'autres articles du présent numéro de «L'Expert-comptable suisse» que l'approche d'audit moderne est aujourd'hui orientée risques, en incluant tout d'abord une analyse des risques d'affaires de l'entreprise auditée et en second lieu des risques d'audit.

Le principal profit que l'entreprise auditée peut tirer de ce processus vient du fait que l'organe de révision communique généralement au client, sous la forme d'une *lettre de recommandations* (*Management Letter*), les faiblesses constatées lors d'une analyse des risques. Bien que ces constatations aient lieu uniquement dans les secteurs de contrôle sélectionnés par le réviseur et se fondent sur des étapes d'audit déterminées de manière tout à fait subjective, elles peuvent donner des indications précieuses au client. La remise d'une lettre de recommandations est facultative; elle n'est obligatoire que dans des cas particuliers, notamment lorsqu'il y a violation de la loi. La *Management Letter* est répandue dans la

plupart des sociétés de révision et comprise dans le mandat d'audit.

Lorsqu'un réviseur décèle un risque qui n'est éventuellement pas (encore) connu de l'entreprise auditée, il le communiquera à l'entreprise de la manière qu'il juge appropriée, mais souvent il le fera oralement.

Bien que cela ne fasse pas directement partie de sa mission légale, le réviseur *sensibilisera* le client au problème et à la nécessité de la gestion des risques. Il existe même des sociétés de révision qui considèrent comme une condition l'existence d'une gestion des risques chez le client et qui l'exigent. L'entreprise doit être en mesure de surveiller de manière régulière et systématique les principaux risques, ce qui a pour but de protéger l'entreprise elle-même mais indirectement aussi de réduire le risque d'audit.

Les sociétés de révision sont souvent aussi à même d'introduire une gestion des risques chez leur client. Cela ne fait bien entendu pas partie du mandat d'audit mais d'un mandat spécial. La société de révision ne cessant ainsi d'améliorer sa connaissance de l'entreprise et de ses structures de risque, le réviseur n'aura dès lors normalement pas de conflits d'intérêts ou de problèmes d'indépendance à surmonter.

Un autre avantage important de l'approche de risque pour l'entreprise révisée est le fait que le réviseur audite en général plusieurs entreprises et qu'il peut dès lors tirer profit de connaissances d'autres sociétés. Souvent, des connaissances générales ou des profils de risque (p. ex. une nouvelle loi) s'appliquent à plusieurs branches. L'entreprise auditée reçoit ainsi des indications précieuses sur les développements actuels. Fournir de telles informations ne représente pas non plus une mission légale impartie au réviseur mais un service qu'il fournit au client.

L'application de l'approche d'audit orientée risques est donc prospective et signifie que le réviseur s'occupe moins de contrôles détaillés, tels les contrôles comptables (que le contrôleur de gestion aura peut être déjà effectués), que de *thèmes d'avenir*. Le management

a ainsi un interlocuteur qui s'occupe moins du passé que de thèmes d'actualité et d'avenir de l'entreprise. La direction et le réviseur parlent la même langue. En Allemagne, le réviseur est même légalement tenu, depuis 1998, «de porter toute son attention sur les problèmes qui peuvent être importants pour le développement futur» [12]. Il en résulte ainsi sans aucun doute une amélioration qualitative de la révision dont profite le client.

Un autre thème est le conseil fourni au client par le réviseur au sujet des répercussions de la présentation des comptes. Il est d'usage que le réviseur réfléchisse à la manière dont les états financiers sont interprétés par les stakeholders, ce qui peut soulever des problèmes ou engendrer des risques. Le réviseur aidera alors à réduire ou à contrôler de tels risques. Souvent, l'actionnaire principal d'une PME n'est même pas conscient de l'influence que peut avoir tel ou tel mode de présentation des comptes. Le réviseur pourra lui donner des explications à cet égard et créer ainsi une plus-value.

En ce qui concerne le risque que les comptes annuels ne concordent pas avec la loi ou les statuts, le réviseur a pour mission légale de procéder à un audit et de délivrer un rapport. A cet égard, il apporte une contribution essentielle à la détection et à la réduction des risques dans le domaine de la régularité.

6. Approche des risques

L'important est que l'entreprise ait une stratégie de risques (synonyme: politique de risques, concept de risques, modèle de risques, processus de gestion des risques, business risk management, etc.), et qu'elle l'applique et la surveille de manière cohérente et pragmatique à la fois.

Il n'appartient toutefois pas à cet article de montrer *comment* l'entreprise applique concrètement la stratégie des risques. Nous renverrons pour ce faire aux autres articles en la matière [13]. Il est un fait aussi que l'introduction d'un processus intégral de risques constitue un projet complexe qui tiendra compte

dans chaque cas des données individuelles.

Compte tenu de la rapidité des cycles de changement, l'introduction de la politique des risques devra tenir compte davantage de visions, de principes et de règles de comportement que d'instructions. Surveiller les risques à l'aide de contrôles sous forme d'instructions directes présente l'inconvénient que ces instructions sont trop rigides et rapidement dépassées face aux variations des risques. L'approche «formation» est elle aussi étroitement liée au contrôle des risques. Mieux les collaborateurs sont formés et familiarisés avec les risques de l'entreprise, meilleur sera le contrôle global des risques.

Comme la politique de risques et les principes, processus et contrôles qu'elle implique entraînent des coûts élevés, il est important que l'entreprise tienne compte du rapport coût/bénéfice. Alors que des risques toujours nouveaux font leur apparition et qu'ils doivent être intégrés dans la politique de risques, il est évident que ceux du passé peuvent ne plus être importants aujourd'hui. Des risques disparaissent ou diminuent aussi parce que l'entreprise a appris à y faire face. Toute entreprise devrait dès lors penser à supprimer des contrôles dépassés. Le principe pourrait être le suivant: «Pour tout nouveau contrôle, nous en éliminons un ancien». Par exemple, on pourrait constater dans une société que le contrôle des cartes de timbrage, exécuté précédemment, n'est plus nécessaire suite à l'introduction d'un nouveau système de bonus orienté sur les projets et qu'il peut être supprimé.

7. Propositions concrètes en vue de contrôler les risques

Les propositions suivantes n'ont pas la prétention d'être systématiques et complètes. Leur but est de donner au lecteur quelques indications pratiques sur les mesures que peut prendre une entreprise pour déceler, gérer et contrôler ses risques. Ces propositions s'entendent notamment pour des structures pas trop complexes, par exemple pour des PME, et pour l'évolution des risques dans le monde actuel des af-

faïres telle qu'elle a été présentée ci-dessus.

- Le principal point mérite d'être rappelé ici: définition d'une *stratégie de risques* intégrale et documentée (identification, évaluation et gestion des risques, c'est-à-dire comment les éviter, les réduire, les surmonter, les contrôler et les surveiller). Les risques qui comportent la somme de dommages la plus élevée sont ceux à traiter en priorité.
- Mise au point et tenue à jour d'un business-plan. Le *business-plan* présente le grand avantage que les dirigeants de l'entreprise doivent se préoccuper de la stratégie, des objectifs et de la manière de les atteindre ce qui augmente durablement les chances de succès. La description de la gestion des risques est une partie intégrante d'un business-plan moderne.
- Constitution d'un *conseil d'administration* compétent, professionnel et responsable. Il arrive encore trop souvent que l'on y renonce soi-disant pour des raisons de coût dans les petites sociétés où le conseil d'administration, la direction et l'actionnaire sont parfois une seule et même personne. Ce qui fait alors défaut dans l'entreprise, c'est la distance nécessaire par rapport aux activités opérationnelles.
- Dans les grandes entreprises et les grands conseils d'administration, on peut constituer des *Audit Committees* qui, en intensifiant la collaboration entre les réviseurs et le conseil d'administration, l'améliorent.
- Choix d'un *organe de révision externe pratiquant l'approche d'audit orientée risques*. Il existe encore de nombreux réviseurs qui travaillent selon l'ancien modèle et sur la base de contrôles détaillés extensifs.
- La création d'un service *d'audit interne* ne semble pas possible pour la plupart des PME, et ce pour des raisons de coût. Mais des activités de *controlling* confiées par exemple au responsable des finances pourraient remplir une fonction similaire. En outre, la société peut également confier de manière ciblée des prestations d'audit interne à un tiers. Cela est encore très rarement le cas sauf s'il existe des exigences légales dans ce sens comme dans les banques ou

chez les négociants en valeurs mobilières.

- La constitution d'une *unité de contrôle des risques* dans certaines entreprises peut se révéler judicieuse bien que cela ne remplace pas l'approche intégrale. Des services tels que des *risk committees* peuvent être créés, comme c'est le cas par exemple dans les banques. Il existe aussi des départements dits de *compliance*, ou un *compliance officer* dans les banques ou dans les grands groupes, qui surveillent le respect des exigences et normes légales, des dispositions des autorités et des règlements internes.
- Des *cours de formation et de perfectionnement* sont profitables pour améliorer sur une base élargie la compréhension de certains risques ou structures de risques auprès du personnel.
- Garantie à l'aide de *produits d'assurance*. Il est étonnant de constater le nombre des prestations d'assurance que l'on peut se procurer actuellement pour se prémunir contre les risques d'affaires. A cet égard, il est recommandé de s'adresser régulièrement à son assureur ou à son courtier. Dans certains cas, on pourra avoir recours à l'assurance ou à la couverture à l'aide de produits financiers (*hedging*).
- *Externalisation (Outsourcing)*: dans l'esprit de transférer des risques sur des tiers, une externalisation peut aider l'entreprise à se concentrer sur ses activités-clés et donc sur ses risques propres;
- *Mesures de sécurité*: ce qui est important, c'est non seulement la sécurité physique des locaux mais aussi la sécurité de l'informatique en général et plus spécifiquement des applications Internet et e-mail.
- Le *reporting de risque* à la direction de l'entreprise et la sensibilisation correspondante du personnel par celle-ci revêtent une importance capitale. Le reporting de risque à la direction et au conseil d'administration ne devrait pas être requis à intervalles trop rapprochés et réguliers car les organes compétents se sentent alors trop déchargés de leur responsabilité.
- *Procédure de benchmarking et de best practice*: cela signifie que des analyses doivent permettre d'opérer des

comparaisons avec les (meilleurs) concurrents. *Participation à des associations professionnelles* pour éviter le cas échéant un certain isolement.

- Introduction d'un processus de gestion de crise et professionnalisation de la fonction de relations publiques, dont l'importance et l'efficacité sont trop souvent sous-estimées par les PME.
- Procéder de façon pragmatique, éviter le formalisme et réduire autant que possible le «papier», mais augmenter les informations de la part du management. Les collaborateurs comprennent ainsi comment et au prix de quels risques l'entreprise peut réaliser son chiffre d'affaires et ses bénéfices et quels sont les risques qui en font ou n'en font pas partie. Ils contribueront alors mieux à atteindre les objectifs de l'entreprise. ■■■

Notes

- 1 Ruud T. Flemming: Integration von Risikomanagement und Interner Revision, exposé au Congrès de l'ASAI à Thoun, le 29 mai 2000.
- 2 Rohner Marcel: Das Risikomanagement im Bankenbereich, exposé au Congrès de l'ASAI à Thoun, le 29 mai 2000.
- 3 cf. Manuel suisse d'audit, Zurich 1998, chapitre 3.
- 4 cf. aussi Barnes Marschdorf Kim, Control Self Assessment: Eine Methode des Risikomanagements, in EC 8/99, p. 693.
- 5 cf. aussi Amhof Roger, Schweizer Markus, Positives Risikomanagement, in EC 8/00, p. 713.
- 6 cf. Association suisse des banquiers: Directives applicables à la gestion des risques en matière de négoce et d'utilisation de dérivés, du 31.1.1996, n° D 45-16.
- 7 Böckli Peter, Schweizer Aktienrecht, Zurich 1996.
- 8 Forstmoser Peter, Meier-Hayoz Arthur, Nobel Peter, Schweizerisches Aktienrecht, Berne 1996.
- 9 Böckli Peter, Corporate Governance auf Schnellstrassen und Holzwegen, in EC 3/00.
- 10 Rohner Marcel: Das Risikomanagement im Bankenbereich, exposé au Congrès de l'ASAI à Thoun, le 29 mai 2000.
- 11 cf. Wyss Hans-Peter, Integriertes Risikomanagement, in EC 3/00, p. 180 et 181.
- 12 cf. Hommelhoff Peter: Die neue Position des Abschlussprüfers im Kraftfeld der aktienrechtlichen Organisationsverfassung, Düsseldorf 1999, p. 115 ss.
- 13 cf. Marschdorf Kim Barnes, Control Self Assessment: Eine Methode des Risikomanagements, in EC 8/99, p. 693 ss; Amhof Roger, Schweizer Markus, Positives Risikomanagement, in EC 8/00, p. 713 ss; Wyss Hans-Peter, Integriertes Risikomanagement, in EC 3/00 p. 179 ss.

Dominik Spiess

Wer profitiert vom risikoorientierten Prüfungsansatz?

Konkrete Vorschläge zu einer verbesserten Risikokontrolle

Dass der risikoorientierte Ansatz der Abschlussprüfung mehr und mehr in den Unternehmungen Einzug hält, ist unbestritten. Davon zeugen auch die verschiedenen Artikel in diesem Heft. Der Autor möchte nun die Frage beleuchten, wem dies letztlich Nutzen bringt. Handelt es sich nur um einen Eigennutzen für den Prüfer, damit dieser seine Arbeit besser, effizienter und mit einem reduzierten Prüfrisiko abwickeln kann? Inwiefern kann auch der Kunde daraus Nutzen ziehen? Welchen Stellenwert hat das Risikomanagement in den Unternehmen? Welches ist dabei die Rolle des Verwaltungsrates? Last but not least gibt der Autor einige praktische Hinweise in Bezug auf das Risikomanagement.

1. Risikodefinition

Das Geschäftsrisiko ist «die Wahrscheinlichkeit, dass ein Ereignis die Fähigkeit einer Organisation, die Geschäftsziele und Strategien erfolgreich zu erreichen, negativ beeinflusst» [1]. Mit Ausnahme von sog. Non Profit Organization (NPO) ist die Gewinnerzielung in den meisten Unternehmungen eines der wichtigsten Unternehmensziele. Das Unternehmensrisiko steht deshalb in engem Zusammenhang mit der Variabilität des Unternehmensgewinns.

Festzuhalten ist zunächst, dass der Gewinn nicht nur eine erstrebenswerte Grösse darstellt, sondern auch von mikro- sowie makroökonomischer Bedeutung ist. Auf Stufe der Unternehmung ist er notwendig, um Aktienkapital oder «Risikokapital» aufzubringen,

die Firma am Start sowie bei der (risikobehafteten) Expansion zu finanzieren, das Kapital und den Wert des Unternehmens aufrecht zu erhalten und über die Dividende zu verzinsen. Die Erwirtschaftung von freiem Cash Flow erlaubt es, weitere Investitionen vorzunehmen, Verschuldungen zurückzuführen, Mitarbeitern Boni zu verteilen, Lohnerhöhungen vorzunehmen, etc.

Von Seiten der Finanzanalysten wird der Wert einer Unternehmung in hohem Mass von deren Kapazität, freien betrieblichen Cash Flow und Gewinn zu erarbeiten, abgeleitet. Dieses Kriterium wurde in letzter Zeit etwas in den Hintergrund gedrängt, indem zahlreiche Start-up-Unternehmungen aufgrund anderer Elemente wie der Innovationskraft, des durchschnittlichen Alters der Mitarbeiter, deren Ausbildung, des Umsatzes oder sogar der sog. «Burn-Rate»,

also des Gegenteils des Gewinns, beurteilt werden. Sogar bei diesen Überlegungen ist die Gewinn-Betrachtung letztlich die relevante, denn die vorgeannten Faktoren sollen wiederum, langfristig betrachtet, die Fähigkeit des Unternehmens, Gewinn zu erzielen, widerspiegeln.

Das inhärente Risiko einer Unternehmung entspricht im Gesamten der Wahrscheinlichkeit, dass sich die Unternehmungsergebnisse auf unvorhergesehene Art und Weise entwickeln. Diese Entwicklung kann sowohl negativ wie auch positiv ausfallen. Wenn die Ergebnisse einer Unternehmung plötzlich um -50% oder um +100% variieren, dann wird die Unternehmung mit einem erhöhten Risiko assoziiert, es sei denn, diese Entwicklung sei vorhersehbar gewesen. Dieses Phänomen kann immer wieder bei den Banken beobachtet werden. Banken weisen derweilen stark schwankende Resultate aus. Oft liegt die Ursache bei den Handelsergebnissen. Die Handelsgeschäfte bei den Banken (Devisen, Wertschriften, derivative Finanzinstrumente, Rohstoffe, etc.) sind den zum Teil wesentlichen Kursschwankungen der entsprechenden Märkte unterworfen. Oft beeinflusst auch die Bildung von Wertberichtigungen auf den durch die Bank eingegangenen Kreditrisiken die Ergebnisse auf unvorhergesehene Art und Weise. Jüngstes Beispiel ist hier die Genfer Kantonbank. Die Markt- und die Kreditrisiken werden aber beispielsweise durch die UBS «bewusst und aktiv, als integraler Bestandteil der Dienstleistungen, eingegangen» [2].

Die meisten Unternehmungen, seien es börsenkotierte oder auch KMU, versuchen, diese Unberechenbarkeit zu reduzieren und das Bild eines sich stetig verbessernden Unternehmens zu

vermitteln. Die Entwicklung der Ergebnisse soll möglichst gleichmässig sein oder zumindest eine gewisse konstante Regel befolgen. Auch das Rechnungswesen und die Rechnungslegungsgrundsätze spielen dabei eine wesentliche Rolle. Dies berücksichtigt auch der Prüfer in seiner Prüfungsstrategie [3].

Die Bemühungen, sich als Unternehmung mit vermindertem Risiko zu präsentieren, rühren daher, dass ein erhöhtes Risiko mit erhöhten Kosten verbunden ist, so zum Beispiel beim Kreditrating der Banken. Noch wichtiger ist aber, dass in der Regel die Stakeholders (Aktionäre, Gläubiger, Mitarbeiter, Staat, Ortsansässige) ein hohes Interesse an einem sicheren Unternehmen haben. Oft ist dies sogar Voraussetzung, um eine Geschäftsbeziehung überhaupt einzugehen. Diese Ausgangslage sollte eigentlich fast zwangsläufig zur Einführung eines umfassenden Risikomanagements Anlass geben. Dem ist aber in der Praxis oft nicht so.

2. Entwicklung und Stellenwert der Risiken

Bei den Geschäftsrisiken möchten wir zwei Kategorien unterscheiden: Erstens die *direkten Geschäftsrisiken*, welche bewusst in Kauf genommen werden und mit welchen die Unternehmung ihr Geld verdient. Das sind diejenigen Risiken, die auch regelmässig eine Chance beinhalten: zum Beispiel geht eine Bank ganz bewusst Kreditrisiken ein, um dadurch mit einer Zinsspanne einen Gewinn zu erwirtschaften. Zweitens die *indirekten Geschäftsrisiken*. Es handelt sich hier um diejenigen, welche in zweiter Linie auf die Unternehmung Einfluss nehmen und nicht im direkten Verhältnis zum Kerngeschäft stehen (z.B. Marketing, Umwelt, Personalwesen, Öffentlichkeitsarbeit) [4]. Wesentlich bei dieser Unterscheidung ist, dass die letzteren in der Regel schlechter wahrgenommen und somit schlechter kontrolliert werden.

Dass sich die Risiken stets verändern und neue Risiken stetig entstehen, ist offensichtlich. Relativ neu ist aber der Rhythmus der Veränderungen und da-

durch das Chancen/Gefahren-Potential. Die Globalisierung der Geschäftswelt, die auch mit der Entwicklung des Internets verbunden ist, bedeutet heute beispielsweise, dass im Tertiärsektor in-nerhalb weniger Monate ein neuer Mitbewerber ins Spiel kommen kann, der unter Umständen aus einer Distanz von Tausenden von Kilometern operiert. Dieser Umstand führt dazu, dass sich den «offenen» Unternehmungen, nämlich denjenigen, die die neuen Möglichkeiten des Internets nutzen, ungeahnte Geschäftsmöglichkeiten bieten. Für deren Mitbewerber entsteht eine gleichermassen intensive Gefährdung der Absatzmärkte.

Diese Beschleunigung des Geschäftslebens hat heute auch beispielsweise zur Folge, dass ein Linien-Manager eines Konzerns durchaus 100–200 E-Mail-Messages pro Tag zu bewältigen hat. Die Chance besteht darin, dass dieser Manager schneller und umfassender wirken kann. Ein unter Umständen neues Risiko besteht darin, dass dieser Manager aufgrund der Fülle der Meldungen, die er erhält, das Wesentliche nicht mehr erkennt. Dieses Beispiel soll auch aufzeigen, dass eine solche Situation beispielsweise vor drei Jahren noch nicht bestand.

Spezifischere und «neuere» Risiken, die heute einen starken Einfluss auf ein Unternehmen haben können, sind

- Neue Gesetze, z.B. zur Produkthaftungspflicht;
- Einfluss der Politik, die Gesetze faktisch ausser Kraft setzt (vgl. nachrichtenlose Vermögen);
- technologische Entwicklungen, Reduktion des Lebenszyklus der eigenen Produkte;
- neue Geschäftspraktiken, wie die Anwendung von erfolgsabhängigen Honoraren oder die vermehrte Anstrengung von Verantwortlichkeitsklagen;
- Umweltrisiken;
- Ruftrisiken, z.B. durch Diffamierung oder durch eine schlecht bewältigte Krise;
- Risiken im Personalwesen, z.B. negative Reaktionen bei einer Kündigung oder umgekehrt eine zu lockere Einstellung bei betrugsähnlichen Vorfällen.

Indem eine Unternehmung nicht nur den direkten Risiken ausgesetzt ist, sondern auch durch indirekte Risiken beeinflusst wird, ohne dies eigentlich zu beabsichtigen, und weil sich diese Risiken schnell verändern können, entsteht ein *Überraschungseffekt*, dem nur mit einer umfassenden Risikostrategie begegnet werden kann. Das bedeutet, dass das Thema «Risiko» integral angegangen werden muss und die wesentlichen Risiken abgedeckt werden sollen.

3. Stand des Risikomanagements in den Unternehmungen

Trotz dieser eigentlich lapidaren Erkenntnis und der umfassenden Literatur ist das Risikomanagement in den meisten Unternehmen nicht integral gelöst. Dies ist nicht nur der Kenntnisstand des Autors aufgrund seiner Wirtschaftsprüfungs- und Beratungstätigkeit, sondern auch eine breitere Erkenntnis [5]. Diese Aussage trifft meistens dann nicht zu, wenn es sich um einen Konzern oder um eine Bank mit einer Internen Revision handelt. Umgekehrt ausgedrückt ist fast immer dort eine umfassende Risikopolitik vorzufinden, wo die Unternehmung über eine Interne Revision verfügt. Diese führt den Risikoprozess des öfters auch bei der Unternehmung ein.

Die direkten Geschäftsrisiken, nämlich diejenigen, die eine Unternehmung willentlich und bewusst eingeht, sind in den profitablen Firmen meist gut kontrolliert. Zu den internen Kontrollen, welche diese überwachen, zählt auch die Interne Revision, die diesen Prozess unterstützt, wie bei den Banken, Effekthändlern und Konzernen. Bei den Finanzinstituten ist der Risikoprozess auch insofern stärker organisiert, als er auf einer rechtlichen Basis sowie im Falle des Handels und beim Einsatz von Derivaten auf einer Richtlinie der Schweizerischen Bankiervereinigung basiert [6].

Indirekte Risiken werden in der Regel schwach wahrgenommen, schlecht kontrolliert. Bei überraschendem Auftreten erfolgt oft eine der Situation

schlecht angepasste Reaktion, weil man eben nicht darauf vorbereitet war.

Aus diesem Grund ist das *Krisenmanagement* mit dem Risikomanagement eng verbunden. Eine Krise tritt insbesondere dann ein, wenn sich das Risiko auf negative Weise realisiert, die Unternehmung schlecht darauf vorbereitet war und sie sich nicht oder nur teilweise darum kümmert. Das Krisenmanagement sollte bei jeder grösseren Unternehmung institutionalisiert sein, was bei einigen Konzernen auch der Fall ist. Besonders ist dabei darauf zu achten, dass die Unternehmung und das operative Business durch die Krise nicht lahmgelegt werden. Bei KMU könnten schon einige wenige Checklisten einen wesentlichen Beitrag zum Krisenmanagement leisten. Griffige Public-Rela-

tions-Regeln bei einer Krisensituation sind des weiteren unabdinglich.

Es soll nicht für jedes nur erkennbare indirekte Risiko ein Überwachungsmechanismus aufgebaut werden; das wäre zu kostspielig. Innerhalb der globalen Risikopolitik sollen aber Grundsätze bestehen, die auch indirekte Risiken ausserhalb des Kerngeschäfts der Unternehmung einschliessen.

4. Rolle des Verwaltungsrates

Der Begriff «Risikomanagement» ist im Schweizerischen Obligationenrecht nicht vorzufinden. Auch ist er im Sachwortverzeichnis der Schweizer Obligationenrechtsspezialisten Böckli [7] sowie Forstmoser/Meier-Hayoz/Nobel

[8] nicht enthalten. Es gibt gegenwärtig in der Schweiz keine expliziten Vorschriften zu diesem Thema. Im Verständnis des Autors fällt die Verantwortung für das Risikomanagement letzten Endes in die Oberleitungsfunktion des Verwaltungsrates gemäss Artikel 716a OR. Dass dadurch im umgekehrten Sinne eine Verantwortung zur Einführung eines Risiko-Systems bestehen könnte, ist jedoch nicht herzuleiten. Allerdings ist es gemäss Böckli [9] «möglich, die Erkenntnisse der internationalen Corporate Governance-Debatte ins Schweizer Recht bruchlos einzuordnen». Böckli vertritt auch die Ansicht, dass das Risikomanagement als einer der Kernbegriffe der Corporate Governance-Debatte angesehen werden kann. Diese Aussagen unterstützen die These, dass das Risikomanagement

sinnmässig zur Oberleitung des Verwaltungsrats gehört. Die Rolle des Verwaltungsrates wird sich aber in den meisten Fällen auf übergeordnete Richtlinien, einen konzeptionellen Rahmen und auf Genehmigungen konzentrieren und die Ausführung des Risikomanagements dem Management überlassen. Das Management sollte für die Auslegung, die regelmässige Anpassung, die Durchführung und die Überwachung des Risikomanagements als voll verantwortlich gelten. Dadurch wird der stark operative Charakter des Risikomanagements ersichtlich. Es wäre deshalb nicht richtig, beim Versagen einer internen Kontrolle die Verantwortung sogleich beim Verwaltungsrat zu suchen. Auch wäre es verfehlt, die Verantwortung für das Risikomanagement bei der Internen oder gar bei der externen Revision anzusiedeln. Risikomanagement ist eine Linien- und nicht eine Stabsaufgabe. Das operative Management wird deshalb auch regelmässig als die verantwortliche Stelle für das Risikomanagement angesehen.

Beispielsweise ist der Verwaltungsrat der UBS für die Genehmigung der Risikomanagement- und Kontrollprinzipien und sind diverse Management-Positionen für die Bewirtschaftung der Risiken verantwortlich [10].

Im Entwurf zum neuen Rechnungslegungsrecht «RRG» bleibt das Risikomanagement unerwähnt. Einzig ist gemäss RRG im Anhang der Jahresrechnung offenzulegen, wie Risiken aus Derivaten überwacht werden (Art. 33 Abs. 3).

Anders ist dies bei den Banken: Da diese im Anhang der Jahresrechnung Erläuterungen zum Risikomanagement geben müssen, ist das Risikomanagement ein bankengesetzliches Erfordernis. Auch bestehen, wie erwähnt, Richtlinien der Bankiervereinigung zu diesem Thema.

Im Ausland [11] ist die Entwicklung weiter fortgeschritten. In Deutschland hat der Vorstand gemäss KonTraG für ein «angemessenes Überwachungssystem» zu sorgen. Die London Stock Exchange verlangt ab Ende 2000, dass dort kotierte Firmen ein angemessenes internes Kontrollsystem unterhalten,

welches der Verwaltungsrat überwachen muss. «The Board should maintain a sound system of internal control».

5. Der Nutzen des risikoorientierten Prüfungsansatzes für das geprüfte Unternehmen

In anderen Beiträgen dieses «Treuhanders» ist umfassend dargelegt, dass der moderne Prüfungsansatz heute auf einer Risikoorientierung basiert, wobei in erster Linie die Geschäftsrisiken des Geprüften und erst in zweiter Linie das eigene Prüfungsrisiko analysiert werden.

Der Hauptnutzen, welchen der Geprüfte aus diesem Prozess ziehen kann, besteht darin, dass die Revisionsstelle dem Kunden in der Regel festgestellte Schwachstellen aus der Risikoanalyse mittels eines sog. *Management Letters* mitteilt. Obwohl diese Feststellungen nur in den vom Prüfer gewählten Prüfungsfeldern gemacht worden sind und auf durchaus subjektiv bestimmten Prüfungsschritten gründen, können sie dem Kunden wertvolle Hinweise geben. Die Abgabe eines Management-Letters ist nur in besonderen Fällen, insbesondere bei Gesetzesverstössen, obligatorisch, ansonsten freiwillig. Bei den meisten Prüfungsgesellschaften ist dieser aber verbreitet und im Prüfungsmandat inbegriffen.

Wenn ein Prüfer ein Risiko erkennt, das möglicherweise der geprüften Unternehmung (noch) nicht bekannt ist, wird er dies der Unternehmung auf angepasste Weise, öfters auch nur mündlich, mitteilen.

Obwohl dies nicht unmittelbar zu seinen gesetzlichen Aufgaben gehört, wird der Prüfer den Kunden auch in Bezug auf die Problematik und die Notwendigkeit des Risikomanagements sensibilisieren. Es gibt sogar Prüfungsgesellschaften, die das Vorhandensein eines Risikomanagements beim Kunden als Voraussetzung ansehen und dieses verlangen. Die Unternehmung soll in der Lage sein, die wesentlichen Risiken regelmässig und systematisch zu überwachen. Dies bezweckt den Schutz der

Unternehmung selbst, aber indirekt natürlich auch eine Reduktion des Prüfungsrisikos.

Prüfungsgesellschaften sind oft auch in der Lage, ein Risikomanagement beim Kunden einzuführen. Dies ist aber sicherlich nicht Bestandteil und Gegenstand des Prüfungs-, sondern eines Sonderauftrages. Da die Prüfungsgesellschaft dadurch die Kenntnis der Unternehmung und ihrer Risikostrukturen nachhaltig verbessert, ergibt sich für den Prüfer in der Regel kein Interessenskonflikt oder Unabhängigkeitsproblem.

Ein anderer wesentlicher Vorteil des Risikoansatzes für die geprüfte Unternehmung ist die Tatsache, dass der Prüfer in aller Regel mehrere Unternehmungen prüft und deswegen Erkenntnisse aus anderen Firmen einbringen kann. Sehr oft sind allgemeine Erkenntnisse oder Risikokonturen (zum Beispiel ein neues Gesetz) für mehrere Branchen relevant. Die geprüfte Unternehmung erhält dadurch wertvolle Hinweise auf aktuelle Entwicklungen. Diese Informationen einzubringen ist aber für den Prüfer wiederum keine gesetzliche Auflage, sondern Dienst am Kunden.

Die Anwendung des risiko- und somit zukunftsorientierten Prüfungsansatzes bedeutet, dass sich der Prüfer weniger mit Detailprüfungen wie zum Beispiel Rechnungskontrollen (die möglicherweise der Controller schon vorgenommen hat), sondern mit *Zukunftsthemen* beschäftigt. Das Management erhält auf diesem Weg einen Ansprechpartner, der weniger Vergangenheitsbewältigung betreibt, sondern sich mit den aktuellen Themen, die die Zukunft der Unternehmung beeinflussen, befasst. Das Management und der Prüfer sprechen dieselbe Sprache. In Deutschland ist der Prüfer seit 1998 sogar gesetzlich verpflichtet, «seine Aufmerksamkeit auf jene Probleme zu lenken, die für die künftige Entwicklung des Unternehmens bedeutsam sein können» [12]. Dadurch entsteht zweifellos eine qualitative Verbesserung der Prüfung, welche dem Kunden zugute kommt.

Ein weiterer Bereich ist die Beratung durch den Prüfer in Bezug auf die Aus-

wirkungen der Rechnungslegung des Kunden. Es ist Usanz, dass der Prüfer Überlegungen anstellt, wie die finanzielle Berichterstattung von Stakeholdern interpretiert wird. Daraus können Probleme oder Risiken abgeleitet werden. Dabei wird der Prüfer einen Beitrag leisten, solche Risiken zu reduzieren oder zu kontrollieren. Sehr oft ist sich ein Hauptaktionär einer KMU gar nicht bewusst, welchen Einfluss diese oder jene Rechnungslegung haben kann. Hier kann der Prüfer aufklären und Mehrwert schaffen.

Was das Risiko, dass eine Jahresrechnung nicht mit dem Gesetz oder den Statuten übereinstimmt, betrifft, hat der Prüfer die gesetzliche Aufgabe, eine Prüfung vorzunehmen und einen Bericht abzugeben. In diesem Sinne leistet er einen wesentlichen Beitrag zur Risikoerkennung und -reduzierung im Bereich der Rechtmässigkeit.

6. Risikoansatz

Wesentlich ist, dass die Unternehmung eine Risikostrategie (Synonyme: Risikopolitik, Risikokonzept, Risikomodell, Risikomanagement Prozess, Business Risk Management u.v.a.m.) besitzt und diese konsequent, aber auch pragmatisch umsetzt und überwacht.

Wie die Unternehmung die Risikostrategie konkret umsetzt, ist nicht Gegenstand dieses Beitrags. Insofern sei auf die diesbezügliche Literatur verwiesen [13]. Auch ist es Tatsache, dass die Einführung eines integralen Risikoprozesses ein komplexes Projekt darstellt, bei dem in jedem Fall die individuellen Besonderheiten berücksichtigt werden müssen.

Bei der Einführung der Risikopolitik sollen aber aufgrund der hektischen Veränderungszyklen vermehrt Visionen, Grundsätze und Verhaltensregeln anstatt Anweisungen verankert werden. Risiken mittels Kontrollen in Form von direkten Anweisungen zu überwachen, hat den Nachteil, dass diese bei Risikoveränderungen zu starr und somit rasch obsolet sind. Eng mit der Risikokontrolle verbunden ist auch der Aus- und Weiterbildungsansatz. Je besser die Mitarbeiter ausgebildet und mit den Risiken der Firma vertraut sind, desto stärker ist die gesamte Risikokontrolle.

Da die Risikopolitik und die damit verbundenen Grundsätze, Abläufe und Kontrollen wesentliche Kosten verursachen, ist es sehr wichtig, dass die Unternehmung die Kosten-Nutzen-Relation beachtet. Obschon stets neue Risiken auftauchen und auch in die

Risikopolitik eingebettet werden sollen, ist es eine Tatsache, dass Risiken der Vergangenheit vielleicht heute gar nicht mehr relevant sind. Risiken entfallen oder vermindern sich auch deshalb, weil die Unternehmung gelernt hat, mit ihnen umzugehen. Jede Unternehmung sollte deshalb auch bedacht sein, veraltete Kontrollen ausser Kraft zu setzen. Der Grundsatz könnte lauten: «Für jede neue Kontrolle eliminieren wir eine alte». Zum Beispiel kann sich in einer Firma herausstellen, dass die bisher ausgeführte Kontrolle von Stempelkarten in der Unternehmung aufgrund eines neuen projektorientierten Bonussystems gar nicht mehr nötig ist und deshalb aufgegeben werden kann.

7. Konkrete Vorschläge zur Risikokontrolle

Mit den nachfolgenden Vorschlägen soll keinerlei Anspruch auf Systematik und Vollständigkeit erhoben werden. Ziel ist es, dem Leser einige praktische Hinweise zu geben, welche Massnahmen eine Unternehmung ergreifen kann, um ihre Risiken zu erkennen, zu bewirtschaften und zu kontrollieren. Dabei verstehen sich die Vorschläge insbesondere für überschaubare Verhältnisse, zum Beispiel in KMU, und

für die oben dargestellte Entwicklung der Risiken in der heutigen Geschäftswelt.

- Der wichtigste Punkt sei hier nochmals erwähnt: Definition einer umfassenden und dokumentierten *Risikostrategie* (Risikoerkennung, -kategorisierung und -bewertung, -bewirtschaftung, d. h. -vermeidung, -verminderung, -Überwälzung, -Kontrolle und Überwachung der Risiken). Dabei müssen vor allem diejenigen Risiken, die eine hohe Schadenshöhe beinhalten, mit Priorität behandelt werden.
- Verfassen und regelmässiges Nachführen eines *Business-Plans*. Die Beschreibung der Risiken ist wichtiger Bestandteil eines Business-Plans. Dieser hat den hauptsächlichsten Vorteil, dass sich die leitenden Stellen mit der Strategie, den Zielen und der Zielerreichung auseinandersetzen und somit die Erfolgchancen nachhaltig erhöhen. Als Nebenprodukt beschäftigt man sich dabei auch mit den Unternehmungsrisiken.
- Konstituierung eines kompetenten, professionellen, verantwortungsbewussten *Verwaltungsrates*. Noch zu oft wird darauf in kleineren Verhältnissen aus sogenannten Kostengründen verzichtet, und der Verwaltungsrat, die Geschäftsleitung und der Aktionär sind ein- und dieselbe Person. Dadurch fehlt in der Unternehmung aber die notwendige Distanz vom operativen Geschehen.
- Bei grösseren Unternehmungen und grösseren Verwaltungsräten können sog. *Audit Committees* eingerichtet werden, welche die Zusammenarbeit mit den Prüfern seitens des Verwaltungsrates intensivieren und so verbessern.
- Wahl einer *externen Revisionsstelle*, die den *risikoorientierten Prüfungsansatz* praktiziert. Es gibt noch zahlreiche Prüfer, die nach altem Muster und aufgrund extensiver Detailprüfungen vorgehen.
- Die Schaffung einer *Internen Revision* scheint für die meisten KMU-Unternehmungen aus Kostengründen nicht möglich. Dabei können aber *Controlling-Tätigkeiten*, die zum Beispiel der Finanzchef ausführt, eine ähnliche Funktion erfüllen. Ausserdem kann die Firma interne Revi-

sionsleistungen auch gezielt einkaufen. Dies ist noch recht selten der Fall, ausser es sei gesetzlich vorgeschrieben wie bei Banken oder Effektenhändlern.

- Obwohl dies den integralen Ansatz nicht ersetzt, kann die Bildung einer *Risikokontroll-Einheit* bei einzelnen Unternehmungen sinnvoll sein. Auch können Gremien wie sog. *Risk Committees* geschaffen werden (wie beispielsweise bei Banken anzutreffen). Bei den Banken oder grösseren Konzernen bestehen auch sog. *Compliance-Abteilungen* oder ein *Compliance Officer*, welche die Einhaltung der Gesetze und sonstigen Vorschriften und behördlichen Auflagen überwachen.
- Um das Verständnis für gewisse Risiken oder Risikostrukturen in der Belegschaft auf breiter Basis aufzubauen, sind *Ausbildungs- und Weiterbildungskurse* von Nutzen.
- Absicherung mittels *Versicherungsprodukten*. Es ist erstaunlich, welche Arten von Versicherungsleistungen heute zur Absicherung von Geschäftsrisiken eingekauft werden können. Hier ist eine regelmässige Anfrage beim Versicherer oder Versicherungsbroker zu empfehlen. In gewissen Fällen kann die Versicherung oder Absicherung auch mittels Finanzprodukten erfolgen (Hedging).
- *Outsourcing*: Im gleichen Sinne der Überwälzung von Risiken auf Dritte kann ein Outsourcing dem Unternehmen dazu verhelfen, bei seinem Kerngeschäft und somit bei seinen eigentlichen Geschäftsrisiken zu bleiben;
- *Sicherheitsvorkehrungen*: Wichtig ist nebst der physischen Sicherheit der Räumlichkeiten vor allem die Sicherheit der EDV allgemein und spezifisch der Internet- und E-Mail-Applikationen.
- Das *Risikoreporting* an die Firmenleitung und die entsprechende Sensibilisierung des Personals durch diese sind von zentraler Wichtigkeit. Das Risikoreporting an die Geschäftsleitung und den Verwaltungsrat sollte nicht in allzu kurzen und regelmässigen Abständen erfolgen, denn sonst fühlen sich die verantwortlichen Stellen zu sehr entlastet.
- *Benchmarking* und *Best Practice-Vorgehen*: Das heisst, mittels ent-

sprechender Analysen den Vergleich mit den (besten) Mitbewerbern anstreben. *Mitwirkung in Branchenverbänden*, um unter Umständen eine gewisse Isolierung zu vermeiden.

- Einführung eines *Krisenmanagement-Prozesses* und Professionalisierung der Public-Relations-Funktion, deren Wichtigkeit und Wirkung von den KMU regelmässig stark unterschätzt werden.
- Pragmatische Vorgehensweise, Vermeidung von Formalismus und möglichst wenig «Papier», dafür ausgiebige *Information durch das Management*. So verstehen die Mitarbeiter, auf welche Weise und mit welchen Risiken das Unternehmen Umsätze und Erträge erwirtschaften kann und welche Risiken dazu oder nicht dazu gehören. Dann werden sie auch einen Beitrag dazu leisten, dass die Unternehmensziele erreicht werden. ■■■

Anmerkungen

- 1 Ruud T. Flemming: Integration von Risiko-Management und Interner Revision, Vortrag an der SVIR-Tagung in Thun, 29. Mai 2000.
- 2 Rohner Marcel: Das Risikomanagement im Bankenbereich, Vortrag an der SVIR-Tagung in Thun, 29. Mai 2000.
- 3 Vgl. Schweizer Handbuch der Wirtschaftsprüfung, Zürich 1998, Teil 3.
- 4 Vgl. auch Barnes Marschdorf Kim, Control Self Assessment: Eine Methode des Risikomanagements, in ST 8/99, S. 693.
- 5 Vgl. auch Amhof Roger, Schweizer Markus, Positives Risikomanagement, in ST 8/00, S. 713.
- 6 Vgl. Schweizerische Bankiervereinigung: Richtlinien für das Risikomanagement im Handel und bei der Verwendung von Derivaten vom 31.1.1996, Nr. D45-16.
- 7 Böckli Peter, Schweizer Aktienrecht, Zürich 1996.
- 8 Forstmoester Peter, Meier-Hayoz Arthur, Nobel Peter, Schweizerisches Aktienrecht, Bern 1996.
- 9 Böckli Peter, Corporate Governance auf Schnellstrassen und Holzwegen, in ST 3/00.
- 10 Rohner Marcel: Das Risikomanagement im Bankenbereich, Vortrag an der SVIR-Tagung in Thun, 29. Mai 2000.
- 11 Vgl. Wyss Hans-Peter, Integriertes Risikomanagement, in ST 3/00, S. 180 und 181.
- 12 Vgl. Hommelhoff Peter: Die neue Position des Abschlussprüfers im Kraftfeld der aktienrechtlichen Organisationsverfassung, Düsseldorf 1999, S. 115 ff.
- 13 Vgl. Marschdorf Kim Barnes, Control Self Assessment: Eine Methode des Risikomanagements, in ST 8/99, S. 693 ff.; Amhof Roger, Schweizer Markus, Positives Risikomanagement, in ST 8/00, S. 713 ff.; Wyss Hans-Peter, Integriertes Risikomanagement, in ST 3/00 S. 179 ff.