

Entrepreneur News

März 2007



Liebe Kunden und Geschäftsfreunde

Corporate Governance und Interne Kontrolle sind Begriffe, welche auch für kleinere und mittlere Unternehmungen enorm an Bedeutung gewonnen haben. Ein kürzlich erschienener Leitfaden «Governance in Familienunternehmen» enthält Empfehlungen für KMU, wie Regelungen und Mechanismen Glaubwürdigkeit, Ver-

trauen und Reputation unterstützen können. Ein neuer Artikel im OR verlangt, dass die Interne Kontrolle künftig schriftlich dokumentiert wird. Lesen Sie auf Seite 4, wie dies KMU am besten anpacken, um sich unnötige Arbeit zu ersparen.

Der Startschuss zum Entrepreneur Of the Year 2007 ist bereits gefallen. Auch dieses Jahr verleiht Ernst & Young den begehrten Titel in drei Kategorien an herausragende Unternehmerpersönlichkeiten. Der einzige nationale Unternehmerpreis nach weltweit einheitlichen Richtlinien wird dieses Jahr in der Schweiz bereits zum zehnten Mal durchgeführt. Im Jubiläumsjahr ist eine Teilnahme besonders interessant – die Bewerbungsfrist für interessierte Kandidatinnen und Kandidaten läuft noch bis am 30. April 2007.

Und nun noch eine Mitteilung in eigener Sache: Nach vielen Jahren bei Ernst & Young werde ich das Unternehmen Ende März 2007 verlassen und in den Ruhestand treten – allerdings bleibe ich weiterhin als Verwaltungsrat sowie als Vorstandsmitglied des Swiss Venture Club für die Wirtschaft aktiv. Ich freue mich sehr, dass unser CEO Prof. Dr. Peter Athanas die Leitung Entrepreneur Markets übernehmen wird.

Ich wünsche Ihnen eine anregende Lektüre.

Peter Bühler

Partner, Leiter Entrepreneur Markets
peter.buehler@ch.ey.com

Gute Governance in Familienunternehmen unterstützt Glaubwürdigkeit, Vertrauen und Reputation

Familienbetriebe beschäftigen in der Schweiz die grosse Mehrheit aller Arbeitnehmenden und bilden damit das Rückgrat der Schweizer Wirtschaft. Von den rund 309 000 Unternehmen in der Schweiz werden 272 000 oder rund 88% von Einzelpersonen und Familien beherrscht oder geführt¹. Umso wichtiger ist in den Familienunternehmen eine gute Governance, deren Regelungen und Mechanismen nachhaltig für Wachstum und Wettbewerbsvorteile sorgen.

Manuel Aeby, dipl. Wirtschaftsprüfer, Partner und Mitglied des Verwaltungsrates, Assurance & Advisory Business Services; manuel.aeby@ch.ey.com

Ungeachtet ihres Anteils wird die Bedeutung der privaten Unternehmen für die Schweizer Wirtschaft oft nur ungenügend wahrgenommen. Ein Grund dafür ist die eingeschränkte Visibilität und Transparenz von Familienunternehmen. Klare Regelungen, offene Kommunikation und eine gute Governance (Definition siehe Kasten Seite 2) geben Ver-

trauen und gewährleisten die Reputation der Familienunternehmen in der Öffentlichkeit.

Im Jahr 2002 hat Economiesuisse Empfehlungen² zur Selbstregulierung für kotierte Unternehmen erlassen, die durch eine Richtlinie der SWX ergänzt wurden. Diese Empfehlungen enthalten jedoch nur wenige spezifische Verhaltensregeln für nicht bör-

Inhaltsverzeichnis

- 1 **Gute Governance in Familienunternehmen unterstützt Glaubwürdigkeit, Vertrauen und Reputation**
Manuel Aeby
- 4 **Neue Regelungen zur Internen Kontrolle: Implementierung in kleinen und mittleren Unternehmen**
Thomas Stenz
- 5 **Informationssicherheit als Antrieb für die Optimierung von Geschäftsprozessen**
Ferdinand Kobelt, David Hyams
- 8 **Seit zehn Jahren sucht Ernst & Young die erfolgreichsten Unternehmerinnen und Unternehmer**
- 8 **Governance bei Pensionskassen**

www.ey.com/ch/entrepreneur

Governance

(aus Wikipedia, der freien Enzyklopädie)

Governance bezeichnet generell das Steuerungs- und Regelungssystem einer politisch-gesellschaftlichen Einheit wie Staat oder Gemeinde. Häufig wird es auch im Sinne von Steuerung oder Regelung einer Institution (etwa einer Gesellschaft oder eines Betriebes) verwendet. Unter Corporate Governance versteht man die Kontroll- und Steuerungsstruktur privatwirtschaftlicher Unternehmen.

senkotierte Familienunternehmen. Diese Lücke wurde nun geschlossen. Private Initianten haben zusammen mit der Vereinigung der Privaten Aktiengesellschaften (VPAG) im November 2006 einen Leitfaden zur «Governance für Familienunternehmen» herausgegeben. Dieser richtet sich an Unternehmer, Verwaltungsräte, Familienmitglieder, Berater und Anwälte. Nachstehend soll dieser Leitfaden kurz vorgestellt werden.

Der Weg zur Good Governance

Die Erzielung von Good Governance in Familienunternehmen ist ein schrittweiser Prozess. Er besteht aus der Verständigung über Ziele und Wege, der Festlegung von Regeln sowie der Etablierung von Strukturen und Kontrollmechanismen. Der Ausgangspunkt dabei ist die Unternehmerfamilie mit ihren Bedürfnissen und Zielen. Family Governance bildet deshalb auch den ersten Teil des Leitfadens. Anschliessende Kapitel sind der Corporate Governance und der Public Governance gewidmet. In jedem Kapitel finden sich die jeweiligen Empfehlungen. Ergänzend ist eine Checkliste beigefügt, anhand welcher der allfällige Handlungsbedarf festgestellt werden kann.

Family Governance: Familienleitbild, Vermögensstrategie und Familienversammlung

Im Kapitel Family Governance werden die Steuerungsmechanismen innerhalb der Unternehmerfamilie beschrieben. Klare Regelungen sorgen hier für die notwendige Stabilität und für ein Umfeld, in dem die Beteiligten ihr Potenzial zu Gunsten der Unternehmung und damit auch der Familie ausschöpfen können.

In einem ersten Schritt ist das *Familienleitbild* zu entwerfen. Es ist eine Zusammenfassung der zentralen Werte und Ziele der Familie einschliesslich der Instrumente zu deren Umsetzung. Es empfiehlt sich, das Familienleitbild schriftlich abzufassen (siehe Kasten).

Das Familienleitbild dient als Grundlage für das *Unternehmensleitbild* und die *Unternehmensstrategie*, welche durch den Verwaltungsrat und die Geschäftsleitung des Unternehmens zu entwickeln sind.

Das Familienleitbild sollte unter den Familienmitgliedern angemessen kommuniziert sowie periodisch überdacht und allenfalls angepasst werden. Die familiären Prioritäten sowie die Geschichte (die Wurzeln) des Unternehmens und seine Zukunft können so aufgearbeitet und an die nächste Generation weitergegeben werden.

In einem weiteren Schritt ist die *Vermögensstrategie* festzulegen. Ziel muss es sein, die persönlichen Bedürfnisse, Vermögenssituationen und Risikoneigungen der einzelnen Beteiligten aufeinander abzustimmen. Ebenfalls ist der Generationenwechsel zu planen. Das Familienunternehmen ist durch Erbteilungen, güterrechtliche Auseinandersetzungen oder Steuern möglichst wenig zu belasten. Das Familienvermögen ist, soweit machbar, vom Geschäftsvermögen zu trennen.

Je nach den Grössenverhältnissen ist die Einführung einer *Familienversammlung* als Organ der gesamten Familie zu empfeh-

Möglicher Inhalt eines Familienleitbildes**Ziele**

- Welche Ziele will die Familie mit der Unternehmung erreichen (Wertmaximierung, Selbstverwirklichung oder Beschäftigungsmöglichkeit für Familienmitglieder)?
- Wer soll am Unternehmen beteiligt sein?
- Welche Rolle soll die Familie im Unternehmen haben?
- Welchen Stellenwert hat das Familienunternehmen innerhalb des familiären Gesamtvermögens?

Werte

- Auf welche Werte ist die Familie stolz?
- Ist die Familie oder die Unternehmung wichtiger?
- Welche Unternehmenskultur soll gelebt werden?

Instrumente

- Wie ist die Familie zu organisieren? Zusammensetzung, Organisation und Aufgaben der Familienversammlung (allenfalls Familienrat); Einbezug der nachfolgenden Generation?
- Wie werden Entscheidungen getroffen? Wie kann das Familienleitbild geändert werden?
- Wie wird innerhalb der Familie informiert? Wie wird gegen aussen informiert?
- Wie soll die Nachfolge geregelt werden?
- Wie wird mit Streitigkeiten umgegangen? Was passiert bei Machtmissbrauch durch ein Familienmitglied? Wer hat das letzte Wort?
- Wie sollen Familienmitglieder behandelt werden, die zur Minderheit gehören oder sich vom Unternehmen trennen möchten?

¹ Frey/Halter/Zellweger, Struktur und Bedeutung von Familienunternehmen in der Schweiz, St. Gallen 2004, S. 5

² Swiss Code of Best Practice for Corporate Governance vom 25. März 2002

len. Deren Mitglieder sind nicht nur die am Unternehmen direkt beteiligten Mitglieder, sondern situativ auch Ehepartner, Nachkommen und die bereits ausgeschiedene Generation. Wichtigste Aufgaben der Familienversammlung sind die Verabschiedung und die periodische Validierung des Familienleitbildes und der Vermögensstrategie. Ferner wird dort über den Geschäftsgang und die künftige Unternehmensentwicklung informiert. In grossen Familien kann es von Vorteil sein, einen Ausschuss zur Familienversammlung – den Familienrat – zu bilden.

Grundlage einer guten Family Governance ist ein aktiver und ehrlicher *Informationsaustausch* unter den Familienmitgliedern. Potenzielle Konfliktsituationen müssen frühzeitig besprochen werden, allenfalls unter Beizug eines externen Moderators. Durch gezielte Information nach aussen erhält die Familienunternehmung in der Öffentlichkeit ein Gesicht und kann so Glaubwürdigkeit und Vertrauen gewinnen.

Die *Nachfolgeregelung* verdient höchste Priorität und ist frühzeitig an die Hand zu nehmen. Deshalb sind familieninterne potenzielle Nachfolger möglichst früh in die Entwicklung des Unternehmens einzu beziehen. Für familieneigene Kandidaten müssen dieselben Anforderungskriterien und Konditionen gelten wie für externe Bewerber. Eine Altersgrenze für den Austritt aus Geschäftsleitung und Verwaltungsrat ist zu empfehlen.

Gute Corporate Governance unterstützt effiziente Leitung und erleichtert Nachfolgeregelung

Das Kapitel Corporate Governance befasst sich mit der zweckmässigen Organisation und den Steuerungsmechanismen im Unternehmen. Primär geht es dabei um das Zusammenwirken zwischen Aktionären, Geschäftsleitung und Verwaltungsrat sowie dem Prüforgan. Ziel ist es, durch Transparenz sowie durch ein ausgewogenes Verhältnis von Führung und Kontrolle das Vertrauen der Eigentümer und weiterer

Anspruchsgruppen zu sichern und damit den nachhaltigen Unternehmenserfolg sicherzustellen.

Grundlage dazu bilden die *Unternehmensstrategie* sowie die *Statuten* und das *Organisationsreglement* der Gesellschaft. Eine auf Best Practice ausgerichtete Corporate Governance sorgt auf dieser obersten Ebene für wirksame Checks and Balances. Im Organisationsreglement ist beispielsweise die Rolle des Verwaltungsrates in Abgrenzung zur operativen Geschäftsleitung klar zu umschreiben. Es ist sicherzustellen, dass er rechtzeitig über alle für die Willensbildung und Überwachung relevanten Aspekte der Gesellschaft informiert wird und über griffige Kontrollinstrumente verfügt. Effizienten Prozessen in der internen Kontrolle, im Risikomanagement und in der Compliance kommt dabei grosse Bedeutung zu.

Eine gute Corporate Governance trägt zu einer effizienten Leitung des Unternehmens bei und hilft einem KMU, auch beispielsweise die kritische Phase der Nachfolgeregelung erfolgreich zu bestehen. Anerkannte Grundsätze der Corporate Governance beeinflussen den Sorgfaltsmassstab, dem ein Verwaltungsrat zu genügen hat. Werden die Grundsätze guter Corporate Governance befolgt, reduziert dies für den Verwaltungsrat das Risiko einer Verantwortlichkeitsklage.

Nicht zuletzt kann eine gute Corporate Governance Zugang zu einer günstigen Finanzierung verschaffen, weil sie Transparenz und Kontrolle an der Unternehmensspitze fördert. Aspekte der Corporate Governance sind bei den bankinternen Ratings von erheblicher Bedeutung und beeinflussen die Kreditkosten. Ebenso beziehen andere Kapitalgeber und Investoren (z.B. im Rahmen eines Unternehmenskaufs) die Corporate Governance regelmässig in ihrer Beurteilung mit ein.

Public Governance bestärkt guten Ruf

Erfolgreiche Unternehmen beschränken sich nicht auf Good Governance im Innenverhältnis. Die enge Zusammenarbeit mit

den Akteuren in ihrem Umfeld macht auch im Aussenbereich entsprechende Steuerungssysteme, die sogenannte Public Governance, notwendig.

Als externe Anspruchsgruppen können *die Kunden, die Mitarbeitenden, die Finanzierungspartner, die Lieferanten* und *die Öffentlichkeit* genannt werden. Ihre Betreuung ist individuell sicherzustellen und die erforderlichen Massnahmen sind im *Umfeldkonzept* festzuhalten. Wo zweckmässig, ist zudem die eigene Haltung zu den verschiedenen Akteuren auch in den familiären und unternehmerischen Leitbild- und Strategiedokumenten zu verankern.

Das Unternehmen ist stets auf seinen *guten Ruf* in der Öffentlichkeit bedacht. Für die Öffentlichkeit ist das Unternehmen in seiner Gesamtheit von Bedeutung. Neben dem wirtschaftlichen Beitrag sind deshalb auch seine sozialen und ökologischen Leistungen von Interesse. Werden Sicherheit und Gesundheit am Arbeitsplatz gefördert, flexible Arbeitsmodelle eingeführt, Sponsoringbeiträge an die Öffentlichkeit geleistet oder wird in der ganzen Wertschöpfungskette auf einen ökologisch sinnvollen Ressourceneinsatz geachtet, können solche Massnahmen das Unternehmensbild und indirekt den finanziellen Erfolg nachhaltig positiv beeinflussen. ■

Der beschriebene Leitfaden «Governance für Familienunternehmen» kann bei der Vereinigung der Privaten Aktiengesellschaften, St. Jakobs-Strasse 7, 4002 Basel, bezogen werden.

Im Laufe der nächsten Monate wird Ernst & Young – in Zusammenarbeit mit dem Swiss Venture Club und der Credit Suisse – Veranstaltungen zum Thema Governance in Familienunternehmen in verschiedenen Schweizer Städten durchführen.

Für Informationen steht Ihnen Esther Guntern, Tel. 058 286 43 28, esther.guntern@ch.ey.com, gerne zur Verfügung.

Neue Regelungen zur Internen Kontrolle: Implementierung in kleinen und mittleren Unternehmen

Neben der Aufteilung der Revision in zwei Arten (ordentliche und eingeschränkte Revision) ist im Rahmen der Änderungen im Revisionsrecht auch eine zusätzliche Aufgabe für die Revisionsstelle bei der ordentlichen Revision in das Gesetz aufgenommen worden. Art. 728a OR (neu) verlangt, dass die Revisionsstelle prüft, dass «ein internes Kontrollsystem existiert». Zusätzlich wird unter Art. 663b OR (revidiert) festgehalten, dass der Anhang zur Jahresrechnung Angaben über die Durchführung einer Risikobeurteilung enthalten muss.

Thomas Stenz, dipl. Wirtschaftsprüfer, Partner und Mitglied des Verwaltungsrates, Präsident der Kommission für Wirtschaftsprüfung der Treuhänder-Kammer; thomas.stenz@ch.ey.com

Nachdem in den ersten Monaten nach der Verabschiedung des Gesetzes durch das Parlament der Wille des Gesetzgebers und damit Art und Umfang dieser Prüfung des internen Kontrollsystems (IKS) zum Teil heftig und kontrovers diskutiert wurden, haben sich die Wogen mit der Zeit geglättet. Niemand in der Schweiz will für nicht kotierte kleinere und mittelgrosse Gesellschaften eine Überreglementierung, wie dies der Sarbanes-Oxley Act in den USA bewirkt hat; auf der anderen Seite kann vom Wirtschaftsprüfer jedoch auch nicht erwartet werden, dass er die Existenz eines internen Kontrollsystems bestätigt, wenn dieses nicht schriftlich dokumentiert ist und in der Praxis nicht gelebt wird. Zusammenfassend haben sich die diversen interessierten Kreise – neben der bereits erwähnten schriftlichen Dokumentation – darauf geeinigt, dass

- der Verwaltungsrat, wie bisher, die Verantwortung für den Umfang und Ausbaugrad des IKS trägt; die Geschäftsleitung die Vorgaben des Verwaltungsrates im Tagesgeschäft umsetzt und, neu, die Revisionsstelle einmal jährlich die Existenz dieses vom Verwaltungsrat definierten IKS bestätigt. Eine Vermischung dieser vom Gesetzgeber klar festgelegten Verantwortungen wäre für alle drei Parteien schlecht;
- es sich bei diesem IKS im Sinne von OR 728a nur um dasjenige handelt, welches eine korrekte und gesetzes- und normenkonforme finanzielle Berichterstattung sicherstellt. Dies schliesst gewisse Bereiche weitergehender interner Kontrolle zwar aus (strategischer Bereich, operative Effizienz), andererseits darf

nicht vergessen werden, dass in aller Regel mehr Unternehmensbereiche zumindest indirekt mit der finanziellen Berichterstattung verbunden sind als nur die eigentliche Finanzbuchhaltung;

- ein IKS-Framework, beispielsweise COSO¹, vom Schweizer Gesetzgeber nicht vorgeschrieben wird; das IKS soll der Grösse und Komplexität des Unternehmens angepasst sein; unter dieser Prämisse ist der Verwaltungsrat frei, Art, Umfang und Ausbaugrad des IKS für sein Unternehmen selber festzulegen.

Anzumerken wäre noch, dass gut geführte und deshalb erfolgreiche Unternehmen in aller Regel bereits über ein – wenn auch oft noch nicht vollständig dokumentiertes – IKS verfügen.

Dokumentation in KMU – praxisorientierte Methode bringt den Erfolg

Wie sollen nun kleinere und mittelgrosse Unternehmen die anerkanntermassen notwendige formelle Dokumentation des IKS vornehmen, damit dessen Existenz schliesslich ab 2008 von der Revisionsstelle auch bestätigt werden kann? Ernst & Young hat zu diesem Zweck eine einfache und praxisorientierte Methodik entwickelt, welche bereits entsprechende Templates und Musterbeispiele umfasst.

Diese praxisbewährte Methode umfasst die folgenden Schritte:

Ausgangslage jeder IKS-Dokumentation ist die Risikobeurteilung durch den Verwaltungsrat. Bei dieser mittels Standardchecklisten geführten Beurteilung ergeben sich

bereits erste wichtige Erkenntnisse darüber, welche Prozessbereiche im Unternehmen (Einkauf, Verkauf etc.) mit Bezug auf das Unternehmensrisikoprofil besonders wichtig sind. Danach legt das Unternehmen fest, welche Prozessbereiche aufgrund der Geschäftstätigkeit des Unternehmens mit Bezug auf die finanzielle Berichterstattung relevant sind. Bei einem typischen Handels- oder Industrieunternehmen sind dies üblicherweise die Bereiche Einkauf/Beschaffung, Verkauf, Personal und die allgemeine finanzielle Berichterstattung sowie, gegebenenfalls, der Produktionsbereich als zusätzlicher Prozess.

Für jeden dieser Prozessbereiche definiert die Unternehmensleitung nun eine Anzahl konkreter und verständlicher IKS-Ziele. Mit Bezug auf den Verkaufsprozess sind illustrativ die folgenden Ziele denkbar:

- Wie stellt das Unternehmen sicher, dass nur Aufträge von Kunden akzeptiert werden, bei welchen die Bonität sichergestellt ist?
- Wie stellt das Unternehmen sicher, dass alle gelieferten Waren oder geleisteten Dienstleistungen zu den korrekten Preisen fakturiert werden?
- Wie stellt das Unternehmen sicher, dass nur von der Unternehmensleitung bewilligte Rabatte und Gutschriften gewährt werden?
- Wie stellt das Unternehmen sicher, dass ausstehende Zahlungen regelmässig gemahnt werden?

Die Erfahrung zeigt, dass in aller Regel nicht mehr als 10 bis 20 solcher konkreter Ziele pro Prozessbereich zu definieren sind, wobei auch hier illustrative Musterziele pro Prozessbereich zur Verfügung stehen.

Sind diese Ziele definiert und vom Verwaltungsrat genehmigt, erfolgt die eigentliche Fleissarbeit: die Dokumentation darüber, mit welchen konkreten Massnahmen

¹ COSO: Committee of Sponsoring Organizations of the Treadway Commission – eine privatwirtschaftliche Organisation in den USA, die helfen soll, Finanzberichterstattungen durch ethisches Handeln, wirksame Interne Kontrolle und gute Unternehmensführung qualitativ zu verbessern.

im Tagesgeschäft das entsprechende Ziel erreicht wird. Die konkreten Massnahmen zur Zielerreichung sind vielfältig und können beispielsweise organisatorischer Natur sein (generelle Gewaltentrennung), manuelle Kontrollen bestimmter Vorfälle umfassen (Zweitvisum) oder automatisierte IT-Kontrollen beinhalten. Die Praxis zeigt, dass entsprechende Kontrollmassnahmen für die meisten IKS-Ziele in den Unternehmen bereits bestehen, es aber etwas Erfahrung braucht, diese zu identifizieren und möglichst konkret und damit in der Praxis prüfbar, schriftlich festzuhalten. Schliesslich erfolgt eine Beurteilung durch die Geschäftsleitung, ob mit den bereits bestehenden und identifizierten Massnahmen das IKS-Ziel erreicht wird oder ob gegebenenfalls Lücken mittels zusätzlich zu definierender Kontrollmassnahmen zu füllen sind. Hier hilft die Erfahrung eines erfahrenen Wirtschaftsprüfers im Projekt, welcher eine Vielzahl anderer Unternehmen kennt, und damit sowohl bei der Identifikation bestehender als auch bei der Definition zusätzlicher Kontrollmassnahmen behilflich sein kann.

Bei der Formulierung der entsprechenden IKS-Ziele gilt es, sowohl die Sicht des Wirtschaftsprüfers oder Finanzdirektors als auch die breiteren Ziele des Unternehmens zu berücksichtigen, damit ein solches Projekt Erfolg hat. Nur so stellt das IKS sicher, dass Fehler in der finanziellen Berichterstattung nicht nur aufgedeckt, sondern bereits im Kern verhindert werden. Daneben sollte die Dokumentation unbedingt bereits bestehende Richtlinien und Reglemente einbeziehen – so kann eine effiziente und praxisorientierte Umsetzung des neuen Gesetzes sichergestellt werden, welche in der täglichen Praxis auch wirklich gelebt wird und in diesem Sinne eben tatsächlich existiert. Werden letzten Endes die am Anfang erwähnten unterschiedlichen Verantwortungen zwischen Verwaltungsrat, Geschäftsleitung und Revisionsstelle beachtet, steht einer erfolgreichen und dem Unternehmen dienenden Einführung eigentlich nichts mehr im Wege. ■

Die neuen Bestimmungen zur Internen Kontrolle – einfach und praktisch umgesetzt Methoden und Erfahrungen aus Schweizer Unternehmen

Ernst & Young führt unter diesem Titel wie folgt Events durch:

Zürich: 18. April 2007

St. Gallen: 23. April 2007

Weitere Veranstaltungen sind geplant in Aarau, Bern, Basel und Luzern – die entsprechenden Daten stehen zurzeit jedoch noch nicht fest.

Für Informationen und Fragen steht Ihnen Esther Guntern, Tel. 058 286 43 28, esther.guntern@ch.ey.com, gerne zur Verfügung.

Informationssicherheit als Antrieb für die Optimierung von Geschäftsprozessen

Informatiksicherheit wird zunehmend als Treiber für die Verbesserung und Optimierung des täglichen Geschäfts erkannt – Unternehmen müssen in diesem Bereich jedoch noch viel aufholen. Dies gilt insbesondere dort, wo das Geschäftsumfeld nicht nur die grössten Chancen bietet, sondern auch die grössten Risiken birgt – dies ist eine der wesentlichen Erkenntnisse des neunten, jährlich publizierten «Ernst & Young Global Information Security Survey»¹. Nachfolgend werden die fünf wichtigsten Faktoren beschrieben, welche für den Erfolg eines Unternehmens besonders kritisch sind. Zudem werden die Antworten der schweizerischen Teilnehmenden mit den weltweiten Ergebnissen verglichen.

Ferdinand Kobelt, dipl. Ingenieur HTL, dipl. Betriebswirtschaftsingenieur HTL/NDS, Partner, Technology & Security Risk Services; ferdinand.kobelt@ch.ey.com

David Hyams, BSc. (Hons.) Comp. Eng., CISSP, Manager, Technology & Security Risk Services; david.hyams@ch.ey.com

Basierend auf der neusten Studie sowie den Ergebnissen der vergangenen Jahre, hat Ernst & Young fünf Prioritäten im Bereich Informatiksicherheit identifiziert. In diesen Bereichen wurden zwar Fortschritte erzielt, es bleibt jedoch ein Bedarf für ständige Verbesserungen bestehen. Konkret handelt es sich dabei um die folgenden Bereiche:

- *Informationssicherheit als Teil der Geschäftsprozesse verankern*, mit entsprechender Ausweitung der Verantwortlichkeiten über die IT-Sicherheitsstelle hinaus;
- *Erhöhung der Bedeutung von Compliance*. Zusätzlich zu den Anforderungen vom Sarbanes-Oxley Act sind für die Schweiz auch die bevorstehenden Ände-

rungen im Obligationenrecht (Art. 633b Pt. 12 und Art. 728), Basel II, Solvency II und MiFID (Markets in Financial Instruments Directive, Richtlinie der EU) besonders relevant;

- *Management der Beziehungen zu den externen Dienstleistern*, um die Herausforderungen und Probleme rechtzeitig zu erkennen und entsprechende Massnahmen zur Risikominimierung einzuleiten;
- *Fokussierung auf den Datenschutz*;

¹ Im Rahmen der neunten «Information Security Survey» wurden 1200 Informatiksicherheitsverantwortliche in 48 Ländern befragt. Aus der Schweiz nahmen 30 Firmen aus 14 verschiedenen Branchen teil.

– *Verbesserung der Informatiksicherheit*, ausgehend von den Sicherheitsvorfällen sowie vom externen Druck durch die IKS-Initiativen.

Einhaltung von regulatorischen und gesetzlichen Anforderungen ist nach wie vor der wichtigste Treiber

Obwohl der Datenschutz ein wichtiges Informatiksicherheitsthema geworden ist, stellt die Einhaltung von regulatorischen und gesetzlichen Anforderungen, wie bereits im Vorjahr, den wichtigsten Treiber mit dem grössten Einfluss auf die Informatiksicherheit dar. Dies wird sich wahrscheinlich auch während der nächsten zwölf Monate nicht ändern. Es besteht eine nachdrückliche Übereinstimmung von fast 80% der Studienteilnehmenden, dass die bereits

unternommenen Aktivitäten zur Erfüllung der regulatorischen und gesetzlichen Anforderungen sich positiv auf die Informatiksicherheit ausgewirkt haben. Es ist diesbezüglich besonders wichtig, dass Unternehmen die Einbettung der Sicherheitskontrollen in die Geschäftsprozesse zwecks Optimierung und Effizienzgewinn proaktiv vornehmen.

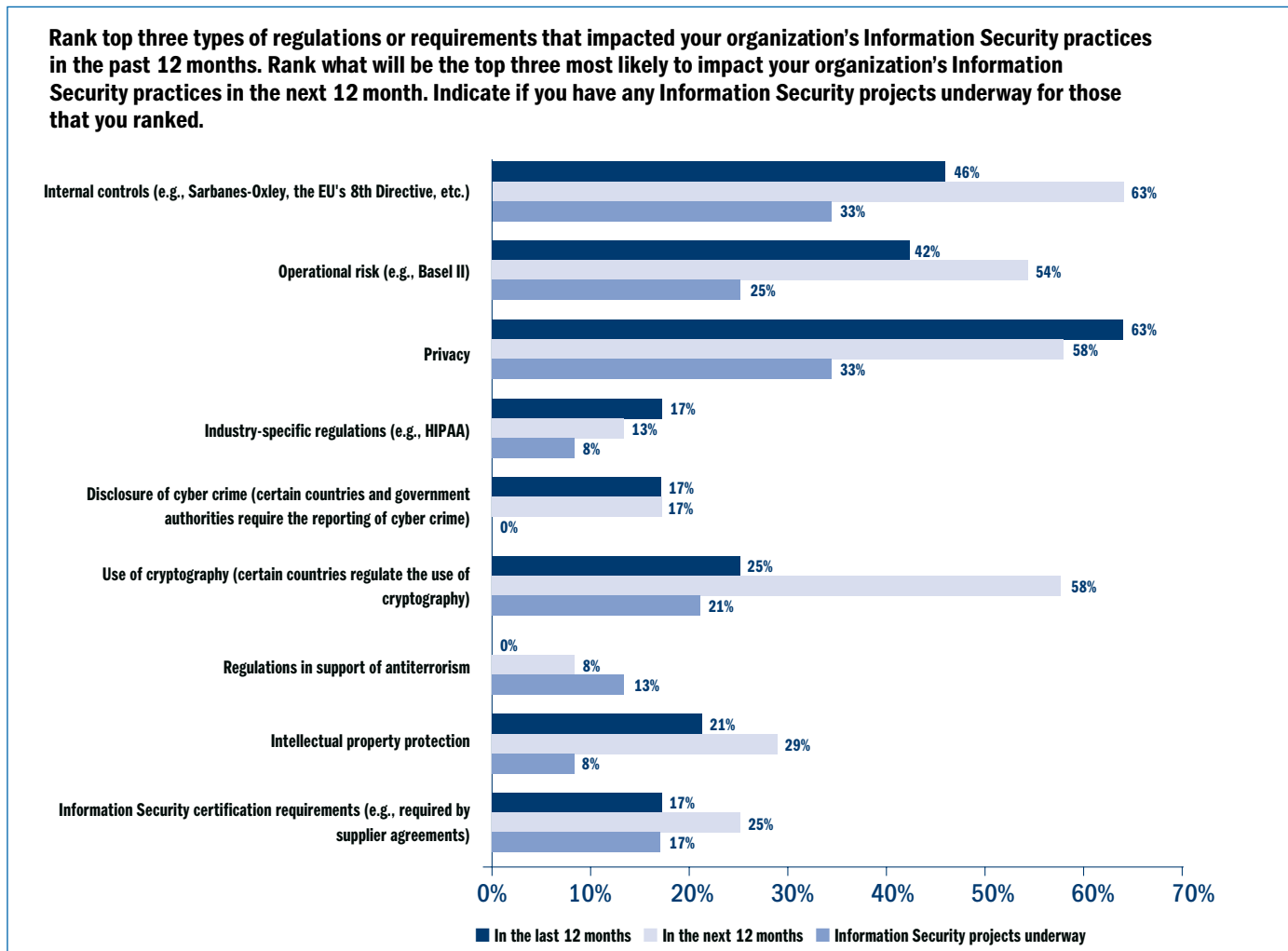
Risiko im Bereich externe Dienstleister

Generell haben Unternehmen die Herausforderungen, die Probleme und die Notwendigkeit von Massnahmen bezüglich der Überwachung von Outsourcern erkannt. Weltweit verfügen mehr als ein Drittel der Studienteilnehmenden über formelle Prozesse für das Risikomanagement von externen Dienstleistern. Dabei verlangen nur 14% der weltweiten Studienteilnehmenden, oder 29% der Antwortenden aus der Schweiz, eine unabhängige Prüfung der Informatik- und Datensicherheit ihrer Lieferanten, beispielsweise mittels SAS-70-Bericht.

menden, oder 29% der Antwortenden aus der Schweiz, eine unabhängige Prüfung der Informatik- und Datensicherheit ihrer Lieferanten, beispielsweise mittels SAS-70-Bericht.

Ergebnisse aus der Schweiz

Obwohl die Schweizer Studienteilnehmenden aus verschiedenen Branchen stammen, bestehen einige wichtige Unterschiede, verglichen mit den globalen Teilnehmenden. Als erstes fällt der relativ hohe Anteil an Antworten aus dem Finanz- und Bankbereich auf, welcher in der Schweiz ca. 50% ausmacht, weltweit lediglich ca. 20%. Zweitens sind fast die Hälfte der Schweizer Studienteilnehmenden global agierende Konzerne. Dieser Anteil ist doppelt so hoch wie bei den ausländischen Teilnehmenden.

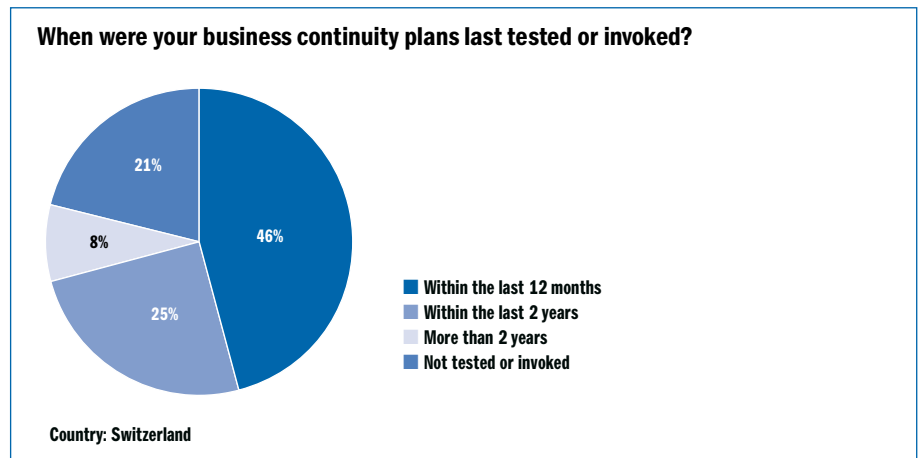


Aufgrund dieser unterschiedlichen Ausgangslage überrascht, dass zum Beispiel 25% der globalen Studienteilnehmenden über einen Informatiksicherheitsbeauftragten verfügen, in der Schweiz jedoch nur 8%. Demgegenüber überrascht eher nicht, dass die Schweizer Teilnehmenden gemäss ihren Antworten viel aktiver sind als ihre ausländischen Kollegen bezüglich Rapportierung von Informatiksicherheitsproblemen an die Aktionäre und andere Investoren. Über die drei Themen «Informatiksicherheitsvorfälle», «Statusberichte über Schlüsselprojekte» sowie «Einhaltung von Sicherheitsanforderungen» informieren doppelt so viele Schweizer Unternehmen regelmässig die Aktionäre als ausländische Firmen. Trotzdem kommunizieren ca. ein Drittel der Schweizer Antwortenden solche Probleme nie.

Auf die Aufforderung, die wichtigsten drei Treiber der letzten zwölf Monate zu nennen, welche die Informatiksicherheit am meisten beeinflusst haben, sind die Antworten der Schweizer Studienteilnehmenden den globalen Antworten sehr nahe, mit Ausnahme der neuen Technologien als wichtigste Treiber. Diese nehmen in der Schweiz mit 38% einen viel höheren Stellenwert ein als weltweit (19%) (vergleiche Grafik Seite 6).

Sowohl die globalen als auch die schweizerischen Studienteilnehmenden betrachten das Interne Kontrollsystem (SOX bzw. Art. 633b Pt. 12 und Art. 728 OR) und den Datenschutz als wichtigste regulatorische und gesetzliche Anforderungen. Aufgrund des hohen Anteils an Finanzinstituten unter den Schweizer Antwortenden ist die Bedeutung der Kryptographie hierzulande dreimal so hoch wie international.

Sowohl die Schweizer als auch die ausländischen Teilnehmenden haben wichtige Fortschritte im Bereich «Business Continuity»-Pläne erzielt – dennoch sind in diesem Bereich weitere Anstrengungen unerlässlich. Denn obwohl fast die Hälfte der Schweizer Antwortenden ihre «Business Continuity»-Pläne während der letzten zwölf Monate getestet haben, haben ca. 20% der Schwei-



zer, die an der Befragung teilgenommen haben, dies noch nie gemacht (siehe oben stehende Grafik).

Ausblick in die Zukunft – Herausforderungen und Prioritäten 2007

Die Studie bestätigt, dass die Informatiksicherheit noch nie so wichtig war wie heute. Sie zeigt, dass viele Unternehmen wichtige Fortschritte bei der Reduktion von Risiken erzielen, indem sie ihre Informatiksicherheit verstärken. Dies kann jedoch nur mit entsprechenden Investitionen, der aktiven Beteiligung der Geschäftsleitung sowie einer ausgereiften Führung der Informatiksicherheit erreicht werden. Aufgrund der dynamischen Natur von Risiken gilt es, die Informatiksicherheitsmassnahmen ständig zu verbessern und anzupassen.

Die Studie hat die folgenden wichtigen Herausforderungen und Prioritäten herauskristallisiert, welche wohl auch in Zukunft Gültigkeit haben werden:

- Aufgrund der Erkenntnis, dass Informatiksicherheitsrisiken stark mit den allgemeinen Geschäftszielen verknüpft sind, wird die Berücksichtigung von Informatiksicherheit an Bedeutung gewinnen.
- Dabei wird die Erfüllung von regulatorischen und gesetzlichen Anforderungen die Informatiksicherheit weiterhin dominieren. Organisationen werden herausgefordert, diese Anforderungen in ihr Risi-

komagement und ihre Interne Kontrolle zu integrieren.

- Der Datenschutz wird für Unternehmen und ihre Informatiksicherheitsverantwortlichen weiterhin von grosser Bedeutung sein.
- Eine Zertifizierung nach anerkannten Standards, typischerweise ISO 27001, wird vermehrt angestrebt.
- Benchmarking, welches auf anerkannten Standards basiert, gewinnt an Bedeutung. ■

Die «Global Information Security Survey» können Sie unter www.ey.com/ch/tsrs herunterladen.

Seit zehn Jahren sucht Ernst & Young die erfolgreichsten Unternehmerinnen und Unternehmer

Entrepreneur Of The Year, der einzige Unternehmerpreis nach weltweit einheitlichen Richtlinien, feiert 2007 in der Schweiz sein zehnjähriges Bestehen. Der Startschuss für die Bewerbung für den diesjährigen Wettbewerb ist bereits gefallen – die Bewerbungsfrist läuft noch bis Ende April 2007. Die Gewinnerinnen und Gewinner erwarten attraktive Preise.

Ernst & Young führt seinen Unternehmerpreis Entrepreneur Of The Year in der Schweiz in diesem Jahr bereits zum zehnten Mal durch – damit handelt es sich bei diesem Preis um einen der ältesten und anerkanntesten der Schweiz in dieser Art. Der strenge, jedoch transparente Auswahlprozess sowie die unabhängige und kompetente Jury gewährleisten, dass die Besten ausserkoren werden. So ist es Ernst & Young immer wieder gelungen, Unternehmer auszuzeichnen, welche auch nach ihrer Auszeichnung sehr erfolgreich waren. Beispiele dafür sind Unternehmer wie Peter Spuhler (Stadler Fahrzeuge AG) oder Dr. h.c. Thomas Straumann (Straumann Holding AG).

Entrepreneur Of The Year hat sich zu einem globalen Programm entwickelt und wird heute in über 40 Ländern der Welt durchgeführt. Die Zusammenarbeit mit den anderen Ländern ermöglicht auch die Durchführung gemeinsamer Veranstaltungen im Rahmen des Programms, von welchen Unternehmerinnen und Unternehmer profitieren und

ihr Netzwerk ausbauen können. So findet zum Beispiel das jährliche «Entrepreneurs Only!»-Wochenende, welches zusammen mit Deutschland und Österreich durchgeführt wird, dieses Jahr in Berlin statt.

Das 10-Jahre-Jubiläum wird am 5. Oktober 2007 im Luzerner KKL gefeiert – es wird nicht nur eine festliche Veranstaltung stattfinden, sondern auch ein Kongress. Schwerpunkte bilden dabei Workshops zu Themen wie Familienunternehmen, Internationalisierung, Finanzierung, Corporate and Personal Governance etc. Höhepunkt dieses Tages bildet der Gala-Abend mit einer Rede von Bundesrätin Doris Leuthard, an welchem die Siegerinnen und Sieger ausgezeichnet werden.

Weitere Informationen zu diesem Programm sowie zu den Teilnahmebedingungen finden Sie unter www.ey.com/ch/eoy. Ausserdem steht Ihnen Brigitte Meyer, Tel. 058 286 36 78, brigitte.meyer@ch.ey.com, gerne für Fragen zur Verfügung. ■

Welche berufliche Vorsorge kann und will sich ein Unternehmen leisten? Governance bei Pensionskassen

Seit dem Inkrafttreten der Loyalitätsbestimmungen des BVG im Januar 2005 ist die Zahl der Vorsorgeeinrichtungen, die sich dem Verhaltenskodex in der beruflichen Vorsorge unterstellen, immer noch unter den Erwartungen. Dieses einzige umfassende Regelwerk im Bereich der Loyalität in der Vermögensverwaltung soll dazu beitragen, dass Vorsorgevermögen ausschliesslich ihrem Zweck entsprechend eingesetzt und Missbräuche bei Anlage und Verwaltung von Vermögen vermieden werden.

Das Anlageverhalten von Pensionskassen und die Loyalität der handelnden Personen steht auf dem Prüfstand. Genügen die Vorschriften des Gesetzes und des Verhaltenskodex oder ist eine zusätzliche Verschärfung der gesetzlichen Rahmenbedingungen notwendig?

Unsere kostenlosen Veranstaltungen geben Ihnen Antworten auf Fragen im Zusammenhang mit der beruflichen Vorsorge und finden wie folgt statt:

- 11. April 2007 in Basel
- 24. April 2007 in Luzern

Für Anmeldungen und weitere Informationen zu dieser Veranstaltungsreihe steht Ihnen Esther Guntern, Tel. 058 286 43 28, esther.guntern@ch.ey.com, gerne zur Verfügung.

Kontakte Regionalleiter

Aarau

Christoph Widmer
christoph.widmer@ch.ey.com
Tel. 058 286 23 72

Basel

Manuel Aeby
manuel.aeby@ch.ey.com
058 286 83 50

Bern

Jürg Scheller
juerg.scheller@ch.ey.com
Tel. 058 286 62 15

Genf/Lausanne

Pierre-Alain Cardinaux
pierre-alain.cardinaux@ch.ey.com
Tel. 058 286 57 82

Lugano

Stefano Caccia
stefano.caccia@ch.ey.com
Tel. 058 286 24 30

Luzern/Zug

Viktor Bucher
viktor.bucher@ch.ey.com
Tel. 058 286 77 26

St. Gallen

Louis Siegrist
louis.siegrist@ch.ey.com
Tel. 058 286 21 31

Zürich

Marco Tagmann
marco.tagmann@ch.ey.com
Tel. 058 286 47 06

Impressum

Entrepreneur News

Newsletter von Ernst & Young AG
Erscheint in deutscher und französischer Sprache

Konzept und Realisation

Ernst & Young AG
Corporate Communications & Marketing
Markus Bernhard und
Anne-Catherine Rüegg
Bleicherweg 21, Postfach, 8022 Zürich
Tel. 058 286 40 85, Fax 058 286 40 50

Abonnemente/Adressänderungen

www.ey.com/ch/newsletter

Gestaltung

Schminke und Team AG, Zürich

© 2007 Ernst & Young

All Rights Reserved.

Ernst & Young is a registered trademark.