

Christian R. Gutzwiller

IT-Risikomanagement und IT-Audit

Ein neues Konzept für die Bewirtschaftung von IT-Risiken

IT-Audit hat im Auftrag und in Zusammenarbeit mit dem IT-Management der UBS AG eine IT-Risikomanagementmethode entwickelt, die es dem IT-Management sowie dem IT-Audit ermöglicht, jederzeit einen Überblick über die aktuellen IT-Risiken zu erhalten. Zudem wird damit das IT Group-Risk Reporting ermöglicht, welches bis auf Konzernleitungsebene pro Quartal auf die wichtigsten IT-Risiken aufmerksam macht.

Diese Risiken werden eng überwacht, bis das einzelne Risiko nicht mehr in dem Ausmass anzutreffen ist, indem es entdeckt wurde und somit im normalen IT-Betrieb bewirtschaftet werden kann. Gleichzeitig können signifikante IT-Audit Feststellungen nach diesem definierten Standard quartalsweise in den IT Group-Risk Report sowie dem IT-Risikomanagement Report einfließen. Damit ist die Voraussetzung geschaffen worden, dass pro Unternehmensbereich, Region, Tochtergesellschaft alle IT-Risiken konsistent und in einer verständlichen Form rapportiert und bewirtschaftet werden. Zudem nützt die Information vom Risikomanagement Report für die Risikoanalyse und für die IT-Auditplanung, die jederzeit für alle zu revidierenden Bereiche demnach risikoorientiert durchgeführt werden kann. In diesem Artikel wird beschrieben, wie das IT-Risikomanagement der UBS AG sich in einer ersten Phase für den Unternehmensbereich Privat und Firmenkunden in der Schweiz entwickelt und wie es seit dem 1.1.99 sukzessive eingeführt wird.

1. IT und IT-Risiken im Blickpunkt der Aufsichtsbehörden

Da sich die Bankenbranche parallel zu technologischen Neuerungen entwickelt, ist IT für alle Banken zu einer entscheidenden Komponente ihrer Geschäftstätigkeit geworden und wird heute von den Aufsichtsbehörden ins-



Christian R. Gutzwiller, Wirtschaftswissenschaftler, Managing Director, Leiter IT-Audit Group, UBS AG, Zürich

besondere in Europa und den USA strengstens überwacht. Der Basler Ausschuss für Banküberwachung (BCBS) und die amerikanische Währungsaufsichtsbehörde (OCC) haben erst kürzlich Richtlinien zum IT-Risikomanagement erlassen.

Das Risikomanagement ist im Bankenbereich von grundlegender Wichtigkeit und Hauptbestandteil unserer Reputation und unseres guten Namens. Bei der Fusion von Schweizerischer Bankgesellschaft (SBG) und Schweizerischem Bankverein (SBV) wurde dem Risikomanagement grosse Bedeutung beigemessen und für die neu entstandene Bank (UBS AG) eine allumfassende Risikopolitik festgelegt. Dank der Richtlinien dieser Politik lassen sich die verschiedenen Bankrisiken gezielt handhaben und die wichtigsten Schlüsselrisiken identifizieren (siehe Abbildung 1). Da die Informatik – meist IT (Information Technology) genannt – nach den Personal- und Immobilienkosten den grössten Investitionsposten darstellt, muss sie sorgfältig überwacht und bewirtschaftet werden. Innerhalb der Risikopolitik kommt dem IT-Bereich daher eine grosse Bedeutung zu.

1.1 Hauptpunkte des IT-Risikos

Um die Risiken im IT-Bereich einzuschränken, müssen folgende zwei Hauptpunkte beachtet werden: Erstens haben die IT-Verantwortlichen dafür zu sorgen, dass für den Bankbetrieb entsprechend leistungsstarke Systeme zur Verfügung stehen. Das ist in einem volatilen Geschäftsumfeld eine anspruchsvolle und nicht immer einfache Aufgabe. Zweitens muss sichergestellt werden, dass trotz aller

Bedeutung der Informatik für die Abwicklung des Kundengeschäfts die Kosten unter Kontrolle bleiben und ein effizienter und effektiver Service zur Sicherung des zukünftigen Wachstums geboten werden kann.

Der IT-Support muss in der Schweiz ungeachtet äusserer Einwirkungen und Schwankungen gewährleistet sein. Bis vor kurzem war der Bereich IT mit der Konsolidierung der Fusion, den Vorbereitungen für den Jahrtausendwechsel und der Einführung des Euro mit erheblichen Herausforderungen konfrontiert. Zusätzlich zu dieser Komplexität muss der IT-Support für die einzelnen Geschäftseinheiten der Bank neue Technologien und Möglichkeiten evaluieren, um das Angebot an innovativen Produkten und Dienstleistungen für die Kunden sicherzustellen (z.B. e-Commerce etc.).

1.2 Handhabung von IT-Risiken

Wer schon an einem Projekt beteiligt war, wo anfänglich eine Liste mit Eventualrisiken erstellt wurde, weiss, dass diese im Verlauf der ersten Projektwochen und mit Voranschreiten des Projekts zunehmend in Vergessenheit gerät und zuletzt wahrscheinlich gar nicht mehr beachtet wird. Ziel der IT-Verantwortlichen und ihres Teams ist es aber, alle Führungsverantwortlichen das Überwachen von Risiken zu lehren und ihnen verständlich zu machen, dass das Diskutieren von erkannten Risiken weder ein Versagen noch eine Schwäche ist.

Es ist wichtig, dass das Risikomanagement zu einem festen Bestandteil des IT-Betriebs wird. Die kontinuierliche Beurteilung von Risiken und das Bestimmen von Entschärfungsmassnahmen

muss Teil der Hauptaufgabe der zuständigen Verantwortlichen sein. Zudem muss sichergestellt sein, dass ein sinnvolles Risikomanagement betrieben wird, welches das einwandfreie Funktionieren des gesamten IT-Bereichs nicht behindert, sondern unterstützt.

1.3 Ziel der IT-Risikoüberwachung – oder: «Warum ist IT-Risikomanagement wichtig?»

Indem IT-Risiken zum ausdrücklichen Bestandteil des IT-Managements werden, lernen die Führungsverantwortlichen die auftretenden IT-Risiken richtig einzuschätzen. Dies ermöglicht der Bank die Einbettung von IT-Risiken in ein kontrolliertes Umfeld und die Sicherstellung einer proaktiven Überwachung.

Abbildung 1
Risikopolitik und -kategorien der UBS im IT-Bereich

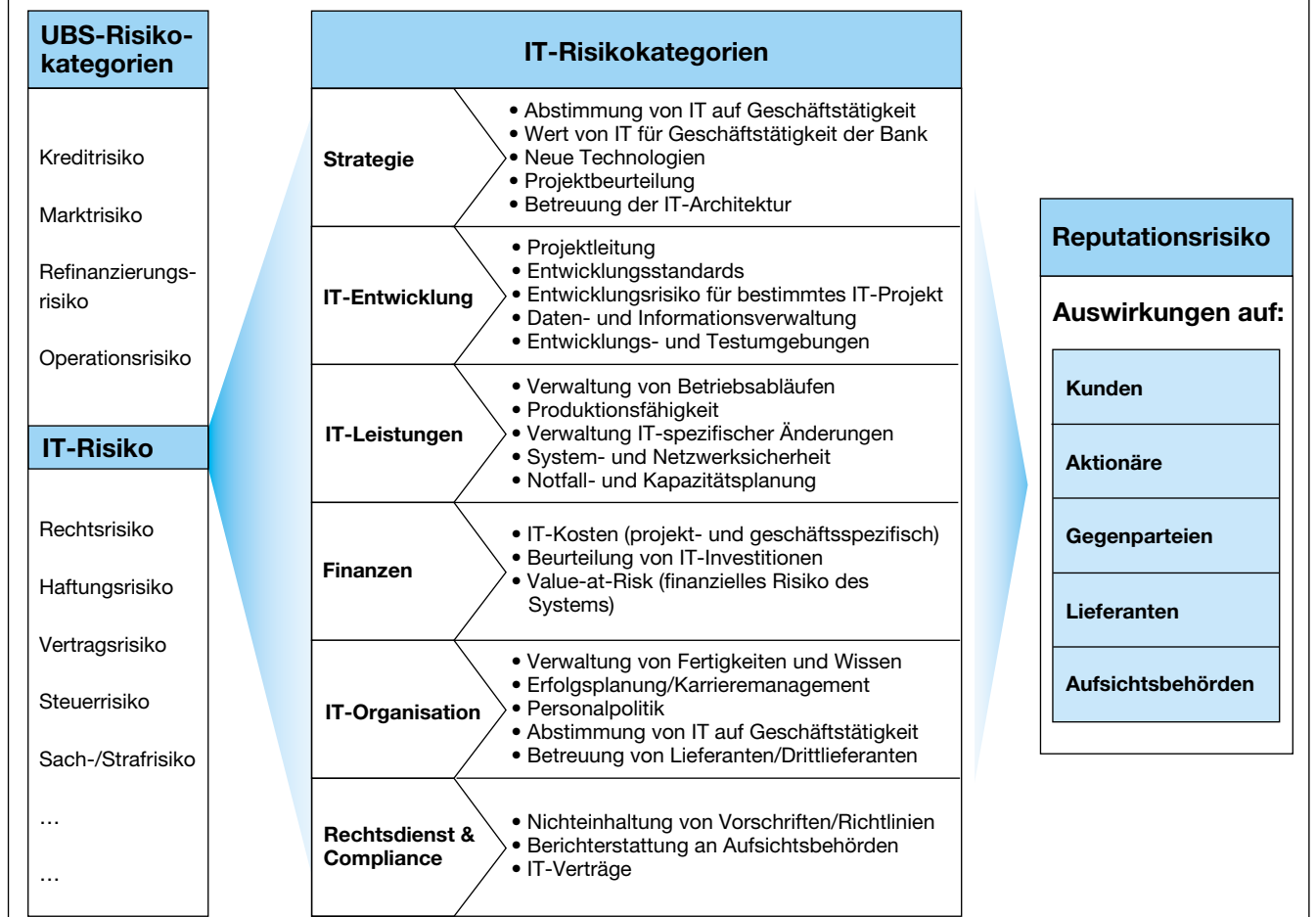
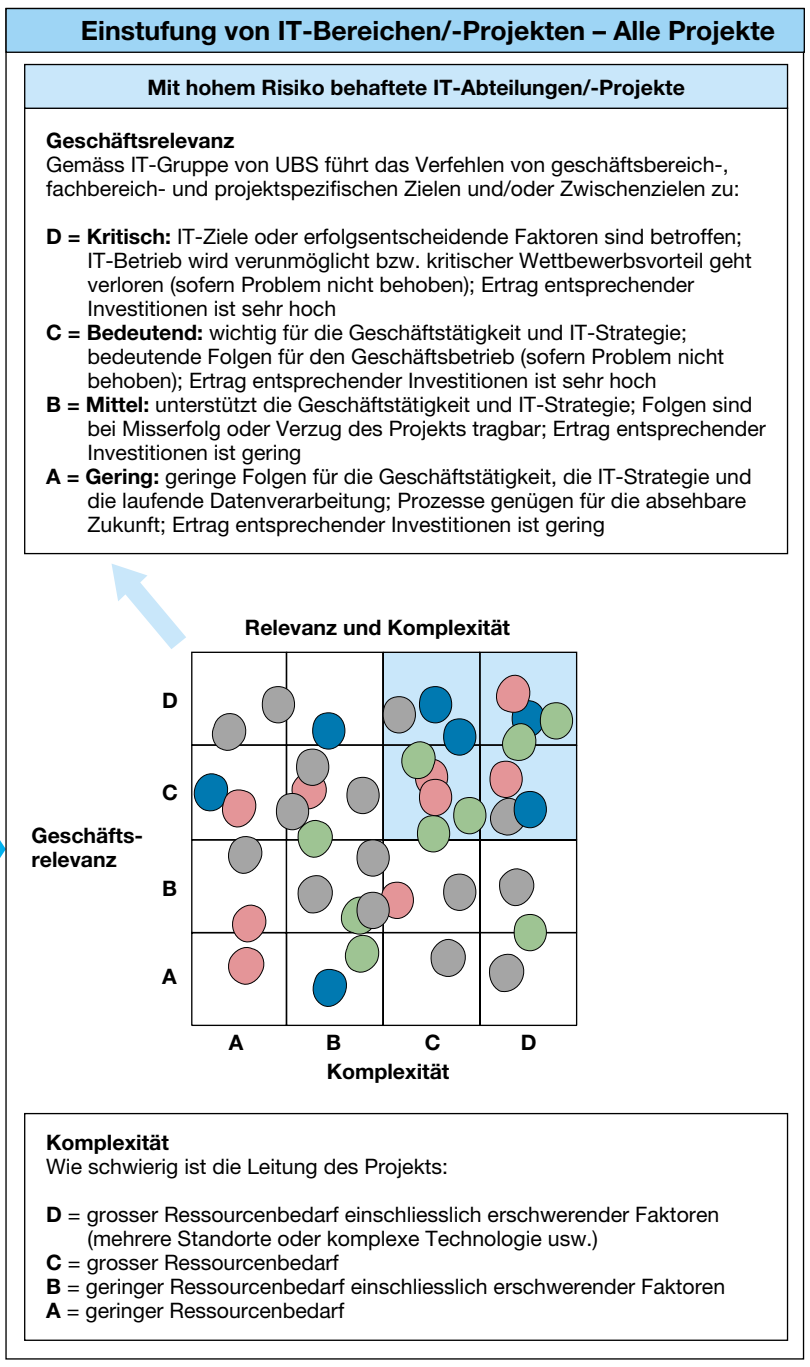


Abbildung 2
Vorbereitende Massnahmen

Projekt-/abteilungsspezif. Kriterien

- «Projekte» werden als solche eingestuft, sobald sie folgende Kriterien erfüllen:
 - Budget von über CHF 500000
 - Bedarf an Ressourcen übersteigt zehn Vollzeitarbeitspensen
 - komplexe Technologie, die an mindestens zwei Standorten eingesetzt wird
- IT-Abteilungen werden vom oberen Management nach der Relevanz der Termine klassifiziert, die sie in der nächsten Berichterstattungsperiode einzuhalten haben.



1.4 Bedingungen für ein erfolgreiches IT-Risikomanagement

Es ist wichtig, dass IT-Risiken mittels entsprechender Richtlinien, die Teil der bankweiten Risikokontrolle sind, konstant überwacht werden. Damit wird garantiert, dass mögliche Auswirkungen auf die Geschäftstätigkeit der Bank erkannt und verstanden werden. Die Führungsverantwortlichen müssen lernen, dass Risiken steuerbar sind.

Um Chancen und Risiken gegeneinander abwägen zu können, bedingt es einer disziplinierten Entscheidungsfindung und Risikobeurteilung. Werden IT-Risikoprozesse in die Geschäftsabläufe der Bank eingebunden, können die IT-Verantwortlichen die Risiken laufend beurteilen und darauf reagieren, bevor irgendwelcher Schaden entsteht. Das IT-Management muss dafür eine flächendeckende Methode entwickeln und sicherstellen, dass diese

zum Bestandteil des gesamten IT-Betriebs wird.

1.5 Schaffen eines klaren Verständnisses für IT-Risiken

Das IT-Management muss von Anfang an klar und einheitlich definieren, was unter der Bewirtschaftung von IT-Risiken zu verstehen ist. Die traditionelle und allgemein übliche Methode des IT-Risikomanagements ist dabei viel zu

technisch und sehr stark auf Sicherheit bedacht. UBS bedient sich einer bedeutend umfassenderen Sichtweise. Da in der heutigen Wirtschaft, die von Informationen geradezu überflutet wird, IT für alle Geschäftsbelange von grösster Bedeutung ist, möchte die Bank IT-Risiken unter einem geschäftsorientierten Blickwinkel angehen. Dafür wurde die folgende umfassende und geschäftsorientierte Definition vereinbart:

«IT-Risiken sind die Unfähigkeit der IT-Organisation, effiziente und wirkungsvolle IT-Lösungen und -Dienstleistungen zur Unterstützung der Bank zur Verfügung zu stellen. IT-Risiken sind die Unfähigkeit, leistungsfähige Systeme und deren Erweiterungen termingerecht zu liefern. IT-Risiken führen zum Verlust oder zu Dateninkonsistenzen und zum Ausfall von Funktionen und Systemen.»

Ein risikoreicher IT-Bereich kann letztlich dem Bankergebnis oder dem Kapital schaden, anstatt dass er ihnen nützt. Die Methode und die Hilfsmittel für das IT-Risikomanagement sollten deshalb den gesamten IT-Lebenszyklus umfassen.

1.6 Konzentration auf IT-Risiken

Bis vor kurzem legte man innerhalb des Fachbereichs IT das Schwergewicht auf die Überwachung folgender Punkte:

- projektspezifische IT-Risiken,
- technische Probleme,
- Einschränkung der Ressourcen,
- Funktionalität.

Dadurch reagierte man im IT-Bereich der Bank grundsätzlich nur auf Risiken, anstatt sich mit ihren Folgen für die zugrunde liegende Geschäftstätigkeit auseinanderzusetzen. Der neue und weitaus umfassendere Ansatz der Bank sieht IT als Grundlage der konzernweiten Risikopolitik an. IT-Risiken werden künftig strategisch angegangen und auch die Auswirkungen auf die Geschäftstätigkeit und den IT-Bereich als Ganzes ausgeleuchtet. Damit lassen sich die Auswirkungen auf die Reputation, die von Gefahren aus dem IT-Bereich ausgehen können, besser erkennen. In Bezug auf Risiken wird der Bereich IT jetzt proaktiv organisiert, wobei die Risikokon-

trolle ein fest darin eingebetteter Prozess ist.

2. Entwicklung eines umfassenden Ansatzes für die Bewirtschaftung von IT-Risiken

Um einen soliden Ansatz für die Bewirtschaftung von IT-Risiken zu entwickeln, mussten die folgenden Punkte definiert werden:

- IT-Risikokategorien,
- Bewirtschaftung von IT-Risiken per se (Abläufe),
- Rapportieren der IT-Risiken (Reporting),
- Leitung des Bereichs IT-Risikomanagement und angegliederter Abteilungen.

Gemeinsam arbeiteten IT-Audit und das IT-Management die Grundlagen für ein effizientes IT-Risikomanagement aus und legten dessen zukünftige Handhabung durch die Bank fest.

2.1 Bestimmen von IT-Risikokategorien

Die Evaluation hat gezeigt, dass es viele Modelle zur Kategorisierung und Klassifizierung von IT-Risiken gibt. Um die für UBS passenden Methoden zur Bestimmung von IT-Risiken zu finden, musste die Arbeitsgruppe eine fachbereichsübergreifende und auf alle Systeme anwendbare Funktionalität sicherstellen. Die verschiedenen Modelle wurden anschliessend im praktischen Umfeld getestet (OCC, BCBS, EIU, vgl. *Legende* am Schluss). Diese Modelle funktionieren in den unterschiedlichsten Betriebsumfeldern wie auch in den Organisationen, wo sie ursprünglich entwickelt wurden und/oder nun Anwendung finden. In der Folge wurden die spezifischen Bedürfnisse von UBS evaluiert und IT-Richtlinien ausgearbeitet, die der Branche und den spezifischen Anforderungen der Bank am ehesten entsprechen. Dabei wurden folgende drei Grundsätze verfolgt:

- *Sämtliche IT-Risiken müssen innerhalb eines Rahmens definiert sein, der den gesamten IT-Lebenszyklus abdeckt.*

- *Sprache und Messung von IT-Risiken müssen für alle Geschäftseinheiten klar verständlich sein.*
- *Die Bewirtschaftung von IT-Risiken muss in die Risikopolitik der Bank eingebunden sein.*

Die IT-Risikokategorien müssen mit den für die gesamte Geschäftstätigkeit der Bank definierten Risikokategorien übereinstimmen und von allen im IT-Bereich von UBS tätigen Mitarbeitern klar verstanden werden. Dazu hat die Arbeitsgruppe eine allgemeine IT-Risikopolitik mit entsprechenden Risikokategorien ausgearbeitet (siehe *Abbildung 1*).

2.2 Abläufe der IT-Risikobewirtschaftung

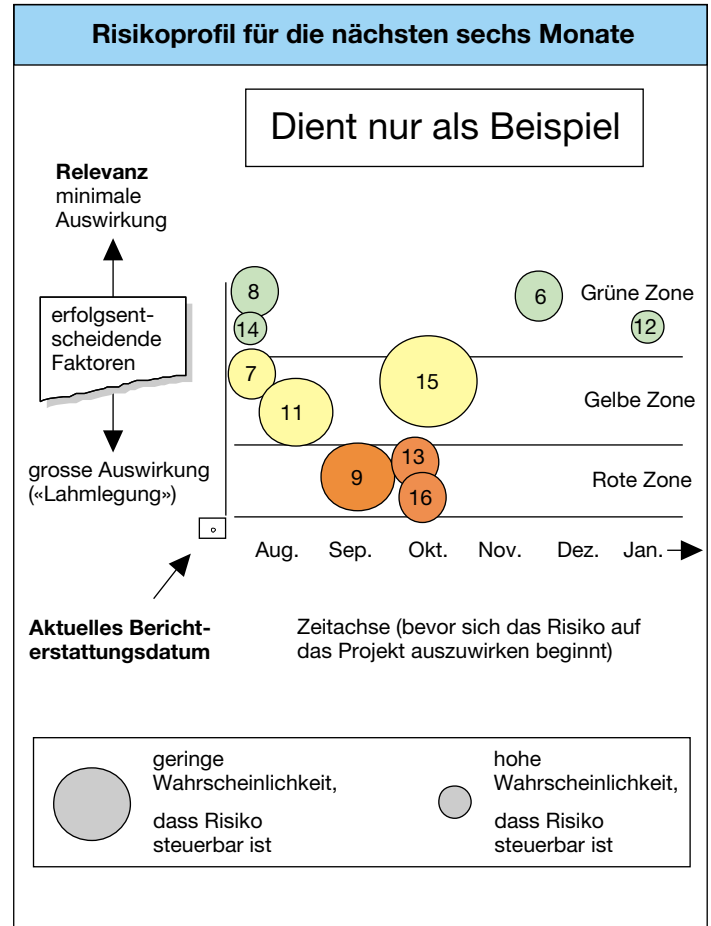
Die Arbeitsgruppe begann als erstes damit, die zur Verwaltung der verschiedenen IT-Risikoaspekte nötigen Hauptschritte festzulegen. Wesentlich dabei ist sicher der Beurteilungsprozess von projekt- und abteilungsspezifischen IT-Risiken sowie die Art und Weise, wie dieser Prozess in den gesamten Lebenszyklus von IT-Projekten integriert wird. Zu Beginn der Bewirtschaftung von IT-Risiken können Projekte und IT-Abteilungen nach ihrer Relevanz für die Geschäftstätigkeit der Bank sowie nach ihrer Komplexität eingestuft werden. Das Hauptgewicht des Risikomanagements (inkl. Befragungen) wird damit auf die wichtigsten Projekte und Abteilungen gelegt.

Die Prioritätensetzung soll gewährleisten, dass für die richtigen Projekte beziehungsweise IT-Abteilungen die entsprechenden Ressourcen bereitgestellt werden und dass den wichtigsten und komplexesten Projekten beziehungsweise IT-Abteilungen die nötige Aufmerksamkeit durch die Führungsverantwortlichen beigemessen wird. Die Prioritätensetzung ist ein sich periodisch wiederholender, kontinuierlicher Prozess, das heisst, nach der ersten Einstufung sind die einzelnen Projekte bzw. IT-Abteilungen regelmässig neu zu beurteilen und einzustufen (monatlich/vierteljährlich, siehe *Abbildung 2*).

Nach der Einstufung erfolgt die Eindämmung der signifikanten Risiken in den wichtigsten Projekten und Bereichen.

Abbildung 3
IT-Organisation Schweiz Risikoprofil (Momentaufnahme)

Geschäftseinheit/ Projekt	Risiken			
	Rot	Gelb	Grün	Gelöst
IT User Services	0(0)	0(1)	3(4)	2
IT Business Services	1(2)	2(3)	0(0)	3
Global Telecom	2(1)	1(0)	1(1)	0
Appl. & Syst. Development	4(2)	0(0)	0(0)	0
RTB Systems Control	0	0(1)	2(5)	1
Appl. Developm. Crp. Ctr.	3(5)	4(4)	0(0)	0
IT Operations (East & West)	2(3)	0(0)	0(0)	2
IT Operations Basel	0(0)	0(0)	4(6)	3
Integration	5(3)	2(2)	1(3)	4
Strategic Solution Program	4(5)	3(2)	0(0)	1
Jahr-2000-Projekt	4(4)	2(5)	2(5)	6
IT-Projekt Euro	4(7)	1(3)	1(3)	7
Total	29	19	14	33



Risiken werden im Rahmen von Gesprächen oder mittels Fragebogen umfassend evaluiert. Der Ablauf ist wie folgt:

- Die hauptverantwortlichen IT- und Projektleiter werden nach IT-Risiken in ihrem Bereich befragt.
- Die Befragungen erfolgen durch speziell im Bereich Risikomanagement ausgebildete, unabhängige Personen.
- Erfahrung in den Bereichen IT und Projektleitung ist dabei Voraussetzung für die Erkennung von versteckten Risiken.
- Einheitliche Messungen werden durchgeführt und die nötigen Hilfsmittel bereitgestellt.
- Dieser Ablauf wiederholt sich periodisch, das heisst, die Hauptverantwortlichen werden regelmässig befragt, damit bestehende Risiken neu überprüft und neue Risiken erkannt werden können.

Mit der so entstehenden Datensammlung wird ein zuverlässiger und umfassender Risikokatalog geschaffen und aufrechterhalten. Dieser ermöglicht die visuelle Darstellung aller in den Projekten enthaltenen Risiken sowie anderer Risiken (z.B. Firewall-Security, und technische Aspekte) auf einer Zeitachse und unterstützt das obere Management in der Diskussion und der Entscheidungsfindung.

Mit einer einfachen, aber effizienten Punktgrafik werden die Führungsverantwortlichen auf die wichtigsten Risiken aufmerksam gemacht (siehe Abbildung 3).

2.3 Rapportierung der IT-Risiken (Reporting)

Nach Abschluss der Befragungen und der Auswertung werden die Ergebnis-

se mittels einer detaillierten Reporting-Struktur zusammengefasst, eingestuft und an die IT-Riskmanager in der IT-Organisation weitergeleitet. Das einheitliche und umfassende Format der Berichte gewährleistet eine ausführliche und einheitliche Terminologie, die in allen IT-Bereichen und -Projekten angewendet werden kann. Sammelberichte decken dabei nicht nur hochgradige Risiken auf, sondern liefern auch jederzeit die nötigen Detailkenntnisse zur Lösung spezifischer Probleme. Weiter erlauben sie dem oberen Management, sich auf die wirklich wichtigen Belange zu konzentrieren und gegebenenfalls dringend benötigten Ressourcen zur Verfügung zu stellen. Die Berichte verkürzen die Reaktionszeit und dienen nötigenfalls der Einleitung von Sofortmassnahmen. Nicht zuletzt fördern sie die Überprüfung von Risiken aus sich überschneidenden Ge-

schäftseinheiten wie auch von Synergien.

Es werden zwei Risikoberichte verfasst: einerseits ein Bericht, der zu Händen des Group-Managements erstellt wird und der den Schwerpunkt auf die wichtigsten Risiken für den Bereich IT legt, und andererseits ein Detailbericht für die IT-Verantwortlichen, der alle abteilungs- und projektspezifischen IT-Risiken auflistet.

Über das bankeigene Intranet (Bankweb) lassen sich die Bewirtschaftung von Risiken und deren Abläufe weitgehend automatisieren, was die Verar-

beitung und Verbreitung massnahmen-spezifischer Informationen wesentlich vereinfacht.

2.4 Zuständigkeiten und Organisation des IT-Risikomanagements

Für das im IT-Risikomanagement tätige Team wurden klare Richtlinien in Bezug auf Verantwortlichkeiten und Zuständigkeiten festgelegt; gleichzeitig wurde auch die passende Eingliederung in die Konzernhierarchie festgelegt. Folgende Verantwortlichkeiten und Zuständigkeiten wurden dabei ermittelt:

- *unabhängige Koordination und Besprechung von IT-Risikoberichten,*
- *Überwachung und Erfassung der wichtigsten Risiken sowie entsprechende Berichterstattung an den Chief Information Officer (CIO) und das obere IT-Management,*
- *Qualitätskontrolle in Bezug auf die Berichterstattung im ganzen IT-Bereich (Einhaltung der Standards),*
- *Förderung eines abteilungsübergreifenden IT-Risikomanagements und Erkennen von Risikoabhängigkeiten.*

Auch das für den Bereich IT-Risiken zuständige *Support-Team* untersteht

RESUME

Gestion des risques informatiques et audit informatique

A la demande de la direction du département informatique d'UBS SA, le service d'audit informatique a développé une méthode de gestion des risques informatiques qui permet, à la fois à la direction du département informatique et au service d'audit informatique, d'être informés à tout moment de la situation en cours et des risques informatiques actuels. De plus, cette méthode permet d'établir un rapport sur les risques dans le domaine informatique (IT Group-Risk Reporting), rapport qui sera distribué une fois par trimestre jusqu'à l'échelon de la direction du Groupe et qui permettra d'attirer l'attention sur les risques informatiques majeurs. Ces risques sont étroitement surveillés jusqu'à ce que chaque risque individuel n'apparaisse plus avec le même degré d'intensité que lors de sa découverte et qu'il puisse être géré par le système d'exploitation informatique traditionnel. Parallèlement, les constatations significatives relevées selon cette méthode par les auditeurs du service informatique peuvent être intégrées une fois par trimestre dans le rapport sur les risques dans le domaine informatique et la gestion des risques informatiques. Les conditions ont donc été créées pour que tous les risques informatiques survenant

dans chaque unité de l'entreprise, chaque région et chaque filiale fassent l'objet d'un rapport et d'une gestion cohérents et harmonisés. En outre, ces informations sont utiles pour l'analyse des risques ainsi que pour la planification des audits informatiques qui peut être réalisée à tout moment en se basant sur les risques dans tous les services qui doivent faire l'objet d'un audit. L'auteur présente le développement de la méthode de gestion des risques informatiques d'UBS SA jusqu'à sa mise en œuvre.

La gestion des risques revêt une importance capitale dans le domaine bancaire et fait partie intégrante de la réputation et de l'image de marque. Lors de la fusion de l'Union de Banques Suisses (UBS) et de la Société de Banque Suisse (SBS), une importance prépondérante a été attribuée à la gestion des risques et, pour la nouvelle banque issue de cette fusion (UBS SA), une politique globale des risques a été élaborée. Grâce aux directives définies par cette politique, il est possible de gérer de manière ciblée les différents risques bancaires et d'identifier les dix risques-clés les plus importants (voir *illustration 1*). Etant donné que l'informatique – généralement désignée par l'abrévia-

tion IT (Information Technology) – arrive à la troisième place des investissements réalisés après le personnel et les immeubles, elle doit faire l'objet d'une gestion et d'un contrôle rigoureux. La politique des risques accorde donc une importance prépondérante au domaine informatique.

Il est primordial que les risques informatiques soient surveillés de manière permanente conformément aux directives contenues dans la procédure de contrôle des risques applicable à toute la banque. Cette manière de procéder permet de faire en sorte que les éventuelles répercussions sur les activités de la banque soient détectées et analysées. La direction doit comprendre que les risques peuvent être gérés. Pour pouvoir évaluer les chances et les risques, il est indispensable que les processus pour la prise de décisions et l'évaluation des risques soient clairement définis. Si les processus relatifs aux risques informatiques sont intégrés dans les méthodes opérationnelles de la banque, les responsables informatiques peuvent évaluer les risques en continu et réagir avant que des problèmes n'apparaissent. La direction du département informatique doit donc développer une méthode globale et

klar definierten Zielen und Kommunikationsrichtlinien:

- Entwicklung und Unterhalt von Richtlinien, Standards und Abläufen,
- Einschätzung von IT-Risiken,
- Durchsetzung einheitlicher Risikoprozesse,
- Aufrechterhaltung der für die Risikobewirtschaftung erarbeiteten Methodik und Berichterstattung zwecks Identifizierung, Überwachung und Kontrolle von IT-Risiken,
- Informieren über projektspezifische Abgabetermine und Verantwortlichkeiten,
- Einreichen von Risikoberichten zu den einzelnen Geschäftseinheiten,

- Diskussion und gegebenenfalls Behebung potenzieller Risiken.

Ein Team zur Überprüfung von IT-Risiken wurde bereits gebildet; es untersteht dem IT-Managementausschuss. Dieses Team überprüft die Risikoberichte des gesamten IT-Bereichs sowie jene der grössten Projekte und bereitet diese für die monatlichen und vierteljährlichen Risikoüberprüfungen vor. Zweck dieser Sitzungen ist:

- Einigung auf die Bewertung sowie die Steuerbarkeit und den Eintretenszeitpunkt eines Risikos,

- Überprüfung des Risikostatus und Erstellung neuer Massnahmenpläne,
- Verabschiedung von Risikoberichten zu Händen des oberen Managements,
- Qualitätskontrolle bei IT-Risikoberichten und -Abläufen.

Legende

- 1 OCC – Office of the Comptroller of the Currency (amerikanische Währungsaufsichtsbehörde)
- 2 BCBS – Basle Committee on Banking Supervision (Basler Ausschuss für Banküberwachung)
- 3 EIU – Economist Intelligence Unit (Geschäftseinheit der englischen Politik- und Wirtschaftszeitschrift «The Economist»)

RESUME

faire en sorte que cette dernière soit intégrée à l'ensemble du système d'exploitation informatique.

Assurer une perception claire des risques informatiques

Dès le départ, la direction du département informatique doit définir de manière claire et harmonisée ce qu'il faut entendre par gestion des risques informatiques. La méthode courante traditionnellement appliquée par la direction informatique est trop technique et très orientée sur les aspects de sécurité. La vision d'UBS se veut nettement plus globale. En effet, dans le contexte économique actuel, les différents acteurs en présence sont littéralement submergés d'informations. L'informatique revêt donc une importance capitale pour toutes les activités de la banque. Cette dernière souhaiterait traiter les risques informatiques en se basant sur une approche orientée sur les différentes activités. Pour ce faire, la définition suivante a été retenue: elle est globale et axée sur les différentes activités de la banque:

«Les risques informatiques sont dus à l'incapacité de l'organisation informatique à mettre à la disposition de la banque des solutions informatiques efficaces et fiables. Les risques informatiques proviennent de l'incapacité à livrer dans les délais impartis des systèmes performants avec leurs extensions. Les risques informatiques aboutissent

à la perte ou à la corruption de données et à des défaillances de fonctions et de systèmes.»

En définitive, un département informatique comportant trop de risques nuit au résultat de la banque ou au capital, au lieu de les soutenir. Par conséquent, la méthode et les moyens utilisés pour la gestion des risques devraient englober le cycle de vie informatique complet.

Développer une approche globale pour la gestion des risques informatiques

Pour pouvoir mettre en place une approche solide permettant d'assurer la gestion des risques informatiques, les points suivants devront être définis:

- catégories de risques informatiques
- gestion des risques informatiques (processus);
- rapport sur les risques informatiques (reporting);
- direction du service de gestion des risques informatiques et services annexes.

Le service d'audit informatique et la direction du département informatique ont élaboré en commun les principes fondamentaux visant à une gestion efficace des risques informatiques et ont défini sa future mise en œuvre au sein de la banque.

Détermination des catégories de risques informatiques

Les catégories de risques informatiques doivent correspondre aux catégories de risques définies pour l'ensemble des activités de la banque et être comprises par tous les collaborateurs travaillant au sein du département informatique d'UBS. A cet effet, le groupe de travail a élaboré une politique générale des risques informatiques indiquant les catégories de risques correspondantes (voir *illustration 1*).

Processus pour la gestion des risques informatiques

En déterminant des priorités, on s'assure ainsi que les moyens nécessaires sont mis à la disposition des projets et des services informatiques qui en ont besoin et que les projets et les services informatiques les plus importants et les plus complexes font l'objet d'une attention suffisante de la part de la direction (voir *illustration 2*).

Grâce au recueil de données ainsi constitué, il sera possible de créer un catalogue des risques fiable et global et de l'actualiser en permanence. Ce dernier permettra la représentation visuelle sur un axe du temps de tous les risques liés à des projets et aidera la direction du groupe dans ses prises de décisions. Un graphique par points simple mais efficace permettra d'attirer l'attention de la direction sur les risques les plus importants (voir *illustration 3*).

CG