

Dr. Anne-Catherine Hahn, L.L.M./Dr. Mark Livschitz  
Dr. Herbert Wohlmann<sup>1</sup>

## Compliance in der Schweiz

	Rn.
I. Übersicht .....	1
II. Ausgewählte Aspekte der Compliance-Elemente .....	5
1. Tone at the Top, Response und Unabhängigkeit der Compliance-Funktion .....	5
2. Risk Assessment .....	10
3. Standards and Controls; Training and Communication .....	13
a) Angemessene Zugänglichkeit und Vermittlung des Compliance-Knowhow ..	13
b) Standards für Produktesicherheits-Compliance .....	14
c) Standards für Antikorruptions-Compliance .....	19
d) Insbesondere: Standards für Zuwendungen und Bewirtungen .....	23
e) Hinreichende Funktionentrennung .....	30
III. Insbesondere Interne Ermittlungen: Übersicht über die rechtlichen Rahmenbedingungen .....	31
IV. Whistleblowing .....	42
V. Blocking Statutes .....	46
1. Verbotene Handlungen für einen fremden Staat (Art. 271 StGB) .....	47
2. Wirtschaftlicher Nachrichtendienst .....	60
VI. Compliance in einigen weiteren wichtigen Rechtsgebieten .....	71
1. Bank und Börse .....	71
2. Insiderregelung .....	72
3. Meldepflichten über Beteiligungen an die Offenlegungsstelle .....	73
4. Pflichtangebot .....	74
5. Ad-hoc-Publizität .....	76
6. Management-Transaktionen .....	77
7. Corporate Governance .....	78
8. Kartellrecht .....	79
9. Arbeitsrecht .....	83
10. Grundstückserwerb .....	85
11. Fazit .....	86

**Arbeitshilfen:** Checkliste Geschenke und Bewirtungen (S 1500 Nr. 1).

### I. Übersicht<sup>2</sup>

**Compliance** (auf Deutsch: Befolgung bzw. Konformität – vorliegend als Befolgung des Rechts bzw. Rechtskonformität verstanden) umfasst die organisatorischen Maßnahmen und internen Abläufe in einem Unternehmen zur Verhinderung von Rechtsverstößen sowie zur Reaktion auf dieselben. Compliance-Maßnahmen wurden für den regulierten Finanzsektor zwecks Bekämpfung von Geldwäscherei seit 1997 im Geldwäschereigesetz (GwG) (Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung im Finanzsektor vom

<sup>1</sup> Dr. Anne-Catherine Hahn und Dr. Herbert Wohlmann sind Rechtsanwälte bei Baker & McKenzie, Zürich. Dr. Mark Livschitz ist selbstständiger Rechtsanwalt in Zürich.

<sup>2</sup> Dieser Abschnitt enthält Auszüge aus Passadelis/Rosenthal/Thür/Livschitz § 18.

10.10.1997, SR 955.0) sowie den dazugehörigen Verordnungen (Geldwäschereiverordnung-FINMA, 8.12.2010, SR 955.033.0; Verordnung über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (GwV) vom 11.11.2015, SR 955.01; Verordnung der eidgenössischen Spielbankenkommission vom 12.7.2007 über die Sorgfaltspflichten der Spielbanken zur Bekämpfung der Geldwäscherei, SR 955.021; Verordnung vom 25.8.2004 über die Meldestelle für Geldwäscherei, SR 955.23) eingeführt. Für Banken, sogenannte „Finanzgruppen und Finanzkonglomerate“ sowie Effektenhändler sind die auf Art. 7 Abs. 1 lit. b FINMAG gestützten FINMA-Rundschreiben 08/21 („Operationelle Risiken Banken“, insb. Rn. 117 ff.) sowie 08/24 („Überwachung und interne Kontrolle Banken“) für Compliance-Belange außerhalb der Geldwäschereibekämpfung ergänzend einschlägig, und zwar in Konkretisierung der sogenannten „Gewährartikel“ (Art. 3 Abs. 2 lit. a BankG und Art. 10 Abs. 2 lit. d BEHG). Ebenfalls gestützt auf Art. 7 Abs. 1 lit. b FINMAG hat die FINMA mittels Rundschreiben 08/32 („Corporate Governance Versicherer“) allgemeine Compliance-Anforderungen für Versicherer und sog. „Versicherungsgruppen und Versicherungskonglomerate“ ausgearbeitet, diesmal in Konkretisierung des versicherungsaufsichtsrechtlichen „Gewährartikels“ (Art. 14 VAG). Für kollektive Kapitalanlagen ergeben sich allgemeine Compliance-Pflichten insb. aus Art. 12a KKV. Ausserdem besteht eine Verpflichtung, zumutbare und notwendige Compliance-Massnahmen zur Verhinderung von Geldwäscherei, Korruptionsdelikten (neu zählt dazu auch die Privatbestechung) Terrorismusfinanzierung und qualifizierter Steuervergehen zu ergreifen.

- 2 Das Bundesgericht hat seit 1970 sukzessive Compliance-Pflichten für Individualpersonen mit beherrschender Stellung im Unternehmen unter dem Titel der sog. strafrechtlichen „Geschäftsherrenhaftung“ entwickelt. Diese Rechtsfigur lässt sich seit 2007 auf Art. 11 StGB (Begehen einer Straftat durch Unterlassen) stützen, wobei sich die Garantienpflicht des Unterlassungstäters aus Art. 11 Abs. 2 lit. d StGB (Schaffung einer Gefahr – Unternehmen als Gefahrenquelle) ergibt. Es handelt sich dabei insbesondere um die Pflicht zur Schaffung einer rechtstreuen Unternehmenskultur durch einschlägige klare Weisungen und Warnungen (heute häufig als „Tone at the Top“ bezeichnet) (BGE 96 IV 155 ff.), Sicherstellung der Konformität gefahrengeneigter Produkte und technischer Vorrichtungen nach den anerkannten Regeln der Technik zur Vermeidung von Körperverletzungen oder gar Tötungen Dritter (BGE 121 IV 10 ff.), die Evaluation von betriebstypischen Deliktsrisiken einschließlich einschlägiger geografischer und Gegenpartei-bezogener Risiken und die entsprechende Anpassung des Unternehmensverhaltens (BGE 122 IV 103 ff.), das Einrichten und Unterhalten eines risikoadäquaten Informations- und Dokumentationsmanagements zwecks Sicherstellung angemessener Prozessabläufe auch in Abwesenheit primär Verantwortlicher, flankiert mit einer „klaren und straffen Organisation“ durch Weisungen und Sicherheitsdispositive (BGE 125 IV 9 ff., 13.). Bei Verdacht eines Rechtsverstoßes hat die Unternehmensleitung sodann die Pflicht, einschlägige Vorgänge und Transaktionen auszusetzen und den Verdacht zu untersuchen (BGE 122 IV 103 ff.). Siehe neuerdings auch BGE 6B\_627/2012, der ganz allgemein bei Auftreten einer nicht ohne weiteres erklärbaren Transakti-

onsanomalie eine Pflicht zu Hintergrundaufklärungen annimmt und einen Pflichtverstoß gleich mit eventualvorsätzlicher Inkaufnahme eines Verbrechens bzw. der Verurteilung wegen Geldwäscherei sanktionieren will. Schließlich hat das Bundesgericht klargestellt, dass Compliance-Pflichten (Garantenpflichten) nicht nur die oberste Unternehmensleitung, sondern durchaus auch Bereichsverantwortliche treffen können (in casu handelte es sich um den Compliance Officer) (*BGE* 136 IV 188 ff.).

Diese bundesgerichtlich postulierten Compliance-Maßnahmen werden in der gegenwärtigen Compliance-Literatur im Wesentlichen auch für Unternehmungen empfohlen und teilweise ergänzt, insbesondere um die Pflicht zur risikoadäquaten Compliance-Überprüfung von Drittparteien, d.h. Nicht-Endbezüger der Unternehmenserzeugnisse in Rechtsbeziehungen zum Unternehmen, wie etwa Agenten, Distributoren, Konsulenten, Lieferanten, zu übernehmende Gesellschaften bei M&A-Transaktionen, etc.; sog. „Third Party Due Diligence“ (s. statt vieler: *Pieth Compliance*, S. 86 ff. und *Harmonizing*, S. 73 ff. und *passim*; *BSK-StGB/Niggli/Gfeller* N 260–305 m.w.N. zu Art. 102 StGB; *Forster* S 229 ff. m.w.N.; vgl. als generisches Hilfsmittel für die risikoorientierte Third Party Due Diligence die Prüfmatrix unter S 1500 Nr. 1 B). Die Notwendigkeit effektiv und risikoadäquat umgesetzter *Third Party Due Diligence* wurde für den Bereich der Antikorruptions-Unternehmenscompliance von der Bundesanwaltschaft im rechtskräftigen Strafbefehl vom 22.11.2011 gegen Alstom Network Schweiz AG sowie der korrespondierenden Einstellungsverfügung gleichen Datums betreffend die Konzernmuttergesellschaft Alstom SA (und in Teilen Alstom Network Schweiz AG) betont. (Strafbefehl Nr. EAII.04.0325 – LEN v. 22.11.2011 gegen Alstom Network Schweiz AG, Erw. 8 ff.; Einstellungsverfügung Nr. EAII.04.0325 – LEN v. 22.11.2011 betr. Alstom SA und in Teilen Alstom Network Schweiz AG, Erw. 2.4. ff.). Die Alstom-Entscheide haben zugleich klargestellt, dass nebst hinreichender Aus- und Weiterbildung risikoexponierter Mitarbeiter und einer hinreichend personell besetzten und vom Geschäftsbetrieb unabhängigen Compliance-Organisation im Unternehmen die adäquate Disziplinierung fehlbarer Mitarbeiter bis hin zu ihrer zivil- und/oder strafrechtlichen Verfolgung ebenfalls zu den notwendigen und zumutbaren Compliance-Maßnahmen nach Art. 102 Abs. 2 StGB gehören kann. (Strafbefehl [op. cit.] Erw. 7 und 15; Einstellungsverfügung [op. cit.] Erw. 1.2.3). Die Verfolgung Fehlbarer auf dem Rechtsweg wurde in der Einstellungsverfügung im Zusammenhang mit mutmaßlicher Bereicherung von Alstom-Mitarbeitern thematisiert. Darüber hinaus ist sie richtigerweise als Compliance-Element nur in Fällen erforderlich, in denen andernfalls keine hinreichende Generalprävention im Unternehmen gewährleistet ist. Ansonsten besteht keine Pflicht zur Beschreitung des Rechtswegs, es sei denn, man unterstehe einer Meldepflicht nach Art. 9 GWG oder Art. 24 bzw. 29 bzw. 36 FINMAG. Ferner dürfte die Beschreitung des Rechtswegs gegen Fehlbare dem Unternehmen helfen, sich auf Wiedergutmachung nach Art. 53 StGB zu berufen. Weitere, spezifische Compliance-Elemente ergeben sich aus der Regulierung des Finanzsektors (dazu oben Rn. 1) für darunter fallende Unternehmen; darauf wird im Laufe dieses Beitrages soweit tunlich später eingegangen.

- 4 Die sich aus den vorgenannten Rechtsquellen ergebenden Compliance-Maßnahmen lassen sich in fünf Maßnahmengruppen bzw. Elementen zusammenfassen: (i) „*Leadership*“ (Führung, verstanden als Prägung einer Unternehmenskultur der Rechtsbefolgung durch die oberste Leitung mittels einschlägiger Weisungen und entsprechenden Vorbildverhaltens; oft auch *Tone at the Top* genannt); (ii) „*Risk Assessment*“ (verstanden als systematische, methodisch konsistente und dokumentierte sowie in tunlichen Zeitabständen wiederholte Erfassung und Bewertung von betriebstypischen Compliance-Risiken); (iii) „*Standards and Controls*“ (risikoadäquate Verhaltensrichtlinien, Prozessbeschriebe und interne Kontrollmaßnahmen auf der Grundlage des *Risk Assessment*); (iv) „*Training and Communication*“ (verstanden als interne Aus- und Weiterbildungsmaßnahmen sowie die Verfügbarkeit Compliance-relevanten Knowhows in den einschlägig risikorexponierten Unternehmensbereichen); (v) „*Oversight and Response*“ (verstanden als vordefinierte Überwachungsprozesse in Gestalt von Stichproben, internen Revisionsroutinen, etc., aber auch vordefinierte reaktive Abläufe bei aufgedecktem Verdacht eines Rechtsverstoßes in Gestalt interner Untersuchungen, arbeitsrechtlicher Disziplinierungsmaßnahmen sowie eventuell Einleitung externer Rechtsverfahren bei zuständigen Behörden und Gerichten) (Fox The Five Essential Elements of a Corporate Compliance Program – Part I, 7.9.2012, [tfoxlaw.wordpress.com/2012/09/07/](http://tfoxlaw.wordpress.com/2012/09/07/); [www.bakermckenzie.com/corporatecompliance/essentialelements](http://www.bakermckenzie.com/corporatecompliance/essentialelements)). Diese fünf Elemente entsprechen übrigens im Wesentlichen den fünf Elementen der bekannten COSO-Risikopyramide (die zum COSO-Risikomanagementwürfel weiterentwickelt wurde) (s. statt vieler [www.aufbewahrungspflicht.de/IKSICS/IKSICS.htm](http://www.aufbewahrungspflicht.de/IKSICS/IKSICS.htm)).

## II. Ausgewählte Aspekte der Compliance-Elemente

### 1. Tone at the Top, Response und Unabhängigkeit der Compliance-Funktion

- 5 Häufig als *Soft Factor* belächelt, wird die Bedeutung dieses Compliance-Elements (zum Stellenwert in der Bundesgerichtspraxis s. unter Rn. 2 m.w.N.) signifikant unterschätzt. Es handelt sich in Wirklichkeit um das wichtigste Compliance-Element überhaupt. Unternehmen mit nahezu perfekten Compliance-Systemen auf dem Papier (sog. „Papier-Compliance“) leiden nicht selten bereichsweise unter systematischer unternehmensinterner Delinquenz, weil Compliance für die oberste Geschäftsleitung nicht an erster Stelle auf der Prioritätenliste steht und mithin besagte Geschäftsleitung nicht oder nicht hinreichend glaubwürdig vermittelt, dass Rechtsbrüche nicht toleriert werden. Betriebssoziologische Untersuchungen zeigen wiederholt, dass die Einstellung der obersten Geschäftsleitung die ganze Unternehmenskultur und mithin auch die Einstellung zur Befolgung relevanter Rechtsvorschriften determiniert, da der weitaus größere Teil der Belegschaft sich als sog. „Mitläufer“ der Unternehmenskultur des Arbeitsumfeldes und damit letztlich der diesbezüglichen Prägung seitens der obersten Leitungsorgane anpasst (s. z.B. *KPMG Fehlverhalten & Ethik am Arbeitsplatz in der Schweiz, 2012*, [www.kpmg.com/CH](http://www.kpmg.com/CH) unter Bibliothek).

Zum richtigen *Tone at the Top* gehören nicht nur die schon 1970 vom Bundesgericht geforderten unmissverständlichen Warnungen, das Recht zu befolgen, sondern auch die effektive Durchsetzung der zugrundeliegenden Weisungen (wie das Bundesgericht ebenfalls betont hat). Dies setzt voraus, dass Verstöße unmissverständlich und konsistent geahndet werden, und dass die Ahnung – soweit arbeitsrechtlich zulässig – im Unternehmen bekannt wird und in *lessons learned* – Diskussionen aufgegriffen wird. Nicht selten haben Unternehmen Hemmungen, verantwortliche Leitungspersonen zu disziplinieren, weil diese für den Umsatz „zu wichtig“ sind; stattdessen sucht man ein subalterneres Bauernopfer. Klassisch ist etwa die Entlassung des lokalen Finanzdirektors, während der eigentlich hauptschuldige Geschäftsführer über jegliche Kritik erhaben bleibt. Der richtige *Tone at the Top* hängt also direkt mit dem Element der *Response* (oben Rn. 3) zusammen. Diese muss unabhängig von Interessen des Linienmanagements erfolgen und wird darum in größeren Organisationen am besten einem vom Linienmanagement unabhängigen Organ übertragen, etwa einem Sanctions Committee, welches direkt dem Verwaltungsrat Bericht erstattet und evtl. auch von einem Verwaltungsratsdelegierten angeführt wird. Häufig lässt sich gerade in größeren Unternehmen nur so bewirken, dass ein hinreichender *Tone at the Top* eine Nulltoleranz gegenüber Compliance-Verstößen durchsetzt, wie dies die Bundesanwaltschaft in dem schon erwähnten Alstom-Fall (Strafbefehl der Bundesanwaltschaft Nr. EAll.04.0325 – LEN v. 22.11.2011 gegen Alstom Network Schweiz AG, Erw. 8 ff.; Einstellungsverfügung Nr. EAll.04.0325 – LEN v. 22.11.2011 betr. Alstom SA und in Teilen Alstom Network Schweiz AG, Erw. 2.4. ff.) gefordert hat.

Der richtige *Tone at the Top* äußert sich außerdem in einer Vielzahl weiterer Indizien: Tritt am Anfang interner Schulungsveranstaltungen ein Mitglied der Geschäftsleitung oder gar der CEO auf und betont, dass Compliance für die Geschäftsleitung zuoberst auf der Agenda steht? Führt das Unternehmen genügend Compliance-Audits durch (sodass jede Einheit innert nützlicher Frist erneut geprüft wird) und bestehen dazu hinreichend interne, ausreichend qualifizierte Revisionsmitarbeiter (Im Alstom-Fall forderte die Bundesanwaltschaft darüber hinaus auch eine genügend große Anzahl hinreichend ausgebildeter und erfahrener Compliance-Mitarbeiter; die Größe der Compliance-Abteilung muss der Größe der Unternehmung angemessen sein.)? Wird der Chief Compliance Officer im Verwaltungsrat regelmäßig begrüßt und einläßlich angehört, oder darf er nur einmal pro Jahr eine zehnmünütige Präsentation herunterleiern? Berichtet Compliance direkt an den Verwaltungsrat (und ist somit ihre Unabhängigkeit vom Linienmanagement in der Unternehmensorganisation abgebildet), oder steht sie (wie leider so häufig noch in der Unternehmenswirklichkeit) organisatorisch unter (statt neben) der Geschäftsleitung? Müssen interne Compliance-Untersuchungen erst vom Linienmanagement bewilligt werden (wobei Einschränkungen des Untersuchungsumfanges regelmäßig gefordert und durchgesetzt werden), oder agiert Compliance diesbezüglich autonom gestützt auf eine Untersuchungs-Richtlinie?

Nicht alle der vorgenannten Indizien müssen vollumfänglich auf Compliance-Freundlichkeit hindeuten. Doch müssen diese in hinreichender Dichte zusammen

mit der kompromisslos zu fordernden Konsistenz punkto *Response* (s. Rn. 6) ein dezidiert Compliance-freundliches Gesamtbild vermitteln. Andernfalls bedarf es nicht selten weitreichender personeller Veränderungen in den höchsten Leitungsetagen eines Unternehmens, um die Unternehmenskultur auf Compliance zu trimmen. Letztlich ist es sehr einfach: Wenn die Geschäftsleitung Compliance will, wird sie im Unternehmen gelebt werden; will sie dagegen keine Compliance oder ist sie ihr gegenüber indifferent, nützen auch die raffiniertesten organisatorischen Maßnahmen nichts.

- 9 Zum richtigen Tone at the Top gehört schließlich, dass der Compliance-Funktion im Unternehmen hinreichende Unabhängigkeit vom Linienmanagement zuerkannt wird. Die Unabhängigkeit der Compliance-Funktion wurde von der Bundesanwaltschaft in den Alstom-Entscheiden (s. Rn. 3) explizit gefordert und ergibt sich auch aus den FINMA-Regularien (s. Rn. 1) für den regulierten Finanzsektor. Dennoch finden sich in der Praxis häufig Bestrebungen des Linienmanagements, Druck auf die Compliance-Abteilung auszuüben und ihren Entscheidungsspielraum einzuengen: Entscheidungsprobleme werde der Compliance-Abteilung in letzter Sekunde unter Hinweis auf die Gefahr großen Umsatzverlustes vorgelegt, gekoppelt mit einer E-Mail von höherer Führungsebene, bitte „mit Augenmaß“ zu entscheiden und das Geschäft nicht zu zerstören; Untersuchungen müssen von Divisionsleitern oder C-Level-Management genehmigt werden, was nur unter Auflagen (sprich: Einschränkungen des Untersuchungsumfanges) geschieht, und dergleichen mehr. Hier ist es wichtig, dass gerade bei Unternehmungen in einer Transitionsphase zu einer robusteren Compliance-Kultur die Unabhängigkeit der Compliance-Funktion organisatorisch flankiert wird, und zwar jenseits der üblichen Berichterstattung des Chief Compliance Officer an den General Counsel oder den CEO. Eine flankierende Maßnahme kann in schwierigen oder noch in Entwicklung befindlichen Compliance-Umfeldern etwa darin bestehen, dass der Chief Compliance Officer Mitglied der Geschäftsleitung wird oder ausschließlich dem Prüfungsausschuss oder Verwaltungsratspräsidenten Bericht erstattet. Der Verwaltungsrat hat nach Schweizer Recht (Art. 716a Abs. 1 Ziff. 5 OR) ohnehin die höchste Compliance-Verantwortung im Unternehmen, sodass sich eine direkte Berichterstattung an denselben oder dessen Ausschüsse mühelos rechtlich untermauern lässt. Natürlich ist es demgegenüber aus Sicht einer optimalen Unternehmensführung zu bevorzugen, dass die Compliance-Funktion dem CEO Bericht erstattet. Zu diesem Zwecke muss aber die Compliance-Kultur eine gewisse Robustheit erreicht haben.

## 2. Risk Assessment

- 10 Compliance-Maßnahmen müssten dem einschlägigen Risikoprofil des Unternehmens angepasst sein und setzten folglich eine Erfassung und Bewertung maßgeblicher, für das betreffende Unternehmen betriebstypischer Rechtsrisiken voraus. So hat das Bundesgericht im Leitentscheid „Von Roll“ (BGE 122 IV 103 ff.) verlangt, dass das Gegenpartierisiko der Kundschaft richtig beurteilt werden müssen (BGE

122 IV 103 ff., 118), und etwa aus dem Umstand, dass Bauteile in den Irak (damals von Saddam Hussein regiert) geliefert wurden, eine erhöhte Gefahr (des Verstoßes gegen Exportbeschränkungen für *Dual Use*-Güter) angenommen werden müsse. Ein Unternehmen muss also nach Bundesgericht die Risiken, die mit seinen Märkten, Kunden und typischen Transaktionsarten verbunden sind (d.h. seine Länder-, Gegenparteien- und Transaktionsrisiken), kennen und angemessen bewirtschaften. Für GWG-regulierte Unternehmen sind Art. 12-14 GwV-FINMA, die ebenfalls nach Gegenpartei-, Länder- und Transaktionsrisiken unterscheiden, sowie die VSB 08 maßgeblich. Danach sind bei Aufnahme einer Geschäftsbeziehung Kundenprofile zu erstellen, wobei der erwartete Umfang, Herkunft und Verwendungszweck der finanziellen Mittel sowie der berufliche und persönliche Hintergrund des Kunden zu eruieren und je nach Risikobewertung von Kunde und Transaktion Hintergrundabklärungen bzw. intensive Transaktionsüberwachungen vorzunehmen. Für Finanzintermediäre besteht sodann eine allgemeine Pflicht zur Feststellung der wirtschaftlichen Berechtigung an Vermögenswerten – auch bei rein operativ tätigen Gesellschaften (Art. 4 GwG).

Ein hinreichendes Risk Assessment muss qualitativ, quantitativ, *top down* und *bottom up* erfolgen. Nicht selten werden in der Praxis Risk Assessment-Interviews schwerpunktmäßig mit dem Management geführt und vor allem dessen Aussagen der Risikoeffassung und -bewertung zu Grunde gelegt. Die Sicht des Managements auf die wahre Risikolandschaft ist indes zuweilen unzulänglich: Zum einen mag es an hinreichender Detailkenntnis der Umstände mangeln; zum andern stellen nicht wenige Manager unbewusst die Situation rosiger dar, als sie wirklich ist, denn wer will schon z.B. Kontrollschwächen in seinem Verantwortlichkeitsbereich wahr haben? Management-Interviews bedürfen daher i.d.R. der Ergänzung durch bottom-up-Gespräche mit subalternen Kräften. Diese können nach qualitativen Kriterien wie z.B. Tätigkeit in Ländern mit niedrigem CPI-Index ([www.transparency.org/cpi2013](http://www.transparency.org/cpi2013)) oder Branchen mit niedrigem BPI-Index ([www.transparency.org/bpi2011](http://www.transparency.org/bpi2011)), oder aber quantitativen Kriterien wie hohen Exportquoten bei grundsätzlich nicht exportorientierten Unternehmen oder hohem Einsatz von Vertriebsmittlern, auffälligen Gutschriftenquoten etc. weit jenseits der üblichen Ausprägung im Unternehmen ausgewählt werden. Die Auswertung quantitativer Auffälligkeiten (die bei Vorhandensein hinreichender ERP-Systeme etwa auch mit einer korrespondierenden Massendatenanalyse einhergehen kann) setzt freilich voraus, dass Benchmarks für normale Transaktionen bzw. für Parameter üblicher Geschäftstätigkeit bestimmt werden können. Grundlage all dieser Erhebungen ist selbstverständlich eine genaue (zu erwerbende) Kenntnis aller Unternehmensabläufe (z.B. auf Grundlage des Studiums eines ggf. vorbestehenden IKS), der Märkte und *Key Performance Indicators* (KPIs) bzw. *Unique Selling Points* (USPs) (ggf. zu erwerben durch Studium des Geschäftsberichtes) etc. Unternehmungen des regulierten Finanzsektors richten sich sodann nach dem FINMA-Rundschreiben 08/21 („Operationelle Risiken Banken“), welches in Rn. 117 ff. detaillierte Anweisungen bzgl. zu bewirtschaftender Risikofelder und notwendige korrespondierende Erhebungen und Bewertungen enthält.

11

- 12 Wesentlich sind bei Risk Assessments sodann zwei weitere Erfordernisse: Das Risk Assessment muss dokumentiert und soll innert angemessener (risikoorientierter) Frist wiederholt werden. Die Robustheit des Risk Assessments und Re-Assessments sollte von der internen und externen Revision periodisch stichprobenbasiert überprüft werden. Vorsicht ist mit zuweilen vorkommenden Self Assessments peripherer Einheiten größerer Konzerne geboten. Die Praxis zeigt hier leider nicht selten, dass vor Ort hinreichend qualifizierte, unabhängige Ressourcen fehlen, um ein verlässliches Abbild der Risikolandschaft zu erzeugen. Auch große Konzerne mit zahlreichen Unternehmenseinheiten kommen nicht umhin, hinreichend qualifizierte Ressourcen zentral bereitzustellen, um die gruppenweiten Risiken verlässlich zu erfassen und folglich zu bewirtschaften.

### 3. Standards and Controls; Training and Communication

#### a) Angemessene Zugänglichkeit und Vermittlung des Compliance-Know-how

- 13 Während bei rechtsgenüßlich durchgeführtem und dokumentiertem Risk Assessments das Formulieren risikoadäquater Standards, d.h. der Compliance-Weisungen des Unternehmens, einigermaßen banal ist, bereiten die hinreichende Kommunikation und Schulung der Inhalte in der Unternehmenspraxis zuweilen Schwierigkeiten. Die bundesgerichtliche Praxis fordert in dieser Hinsicht (*BGE* 125 IV 9 ff., 13- Rothornbahn-Entscheid ) ein adäquates Informations- und Dokumentationsmanagement, um insbesondere auch bei Abwesenheiten primär Verantwortlicher angemessene Prozessabläufe sicherzustellen, und verlangt eine diesbezüglich „klare und straffe Organisation“ durch Weisungen und Sicherheitsdispositive, die eine risikoadäquate Informationsauswertung und -verteilung umfassen müssen. Gerade größere Unternehmen sind daher gut beraten, (i) Prozesse zur Entwicklung, Genehmigung, Aktualisierung und Verbreitung bzw. dem Nachhalten von Weisungen, Policies etc. zu definieren und zu implementieren; (ii) professionell unterhaltene *Houses of Policies* einzurichten und für hinreichenden elektronischen Zugang all derjenigen zu sorgen, die vernünftigerweise Zugang brauchen; (iii) jährlich wiederkehrende, stufengerechte Schulung der Policies durchzuführen, wobei in Risikobereichen bloße *e-learning*s nicht ausreichen dürften.

#### b) Standards für Produktesicherheits-Compliance<sup>1</sup>

- 14 Die Bundesgerichtspraxis hat für den Bereich der Produktesicherheits-Compliance die folgenden Standards hervorgebracht:
- 15 Laut dem „Hebebühne-Urteil“ (*BGE* 121 IV 10) hätte der Geschäftsführer des Verkäuferunternehmens einer Hebebühne, die infolge eines Konstruktionsfehlers die Ladung verlor und so einen Mitarbeiter zu Tode zerdrückte, die Konformität der Hebebühne mit den anerkannten Regeln der Technik sicherstellen müssen. Der

<sup>1</sup> Dieser Abschnitt enthält Auszüge aus *Bühler/Killias/Livschitz* Unternehmensstrafbarkeit und Produktesicherheit, 2013, S. 153 ff.

Geschäftsführer habe diese Pflicht verletzt, indem er vor Auslieferung der Hebebühne keine Endkontrolle durchgeführt hätte. Bei dieser Endkontrolle hätten auch versteckte Mängel entdeckt und geprüft werden müssen. Dem stehe das Fehlen technischer Kenntnisse beim Geschäftsführer nicht entgegen; er hätte sich sachverständig beraten lassen müssen. Fazit: Endkontrollen, die auch versteckte Produktmängel aufspüren, sind risikoadäquat mittels Weisungen anzuordnen, und einschlägige technische Kenntnisse hat man zu haben.

Im „Schachtrahmen-Fall“ (BGE 110 II 456) war einem Arbeiter ein Betonschachtrahmen auf den Fuß gefallen und verursachte beim Arbeiter einen lebenslangen schweren Schaden mit Invaliditätsfolgen. Der Grund für das Herunterfallen des Schachtrahmens war eine bei der Endkontrolle mangelhaft geprüfte Aufhängevorrichtung. Das Bundesgericht stellte klar, dass bei der Endkontrolle nicht bloß das Standhalten einer normalen, sondern auch einer höheren als der normalen Belastung zu prüfen sei. Fazit: Die anzuweisenden Endkontrollen müssen Überbelastungstests vorsehen.

16

Im „Herbizid-Fall“ (BGE 120 IV 300) hatte ein einschlägig verantwortlicher Mitarbeiter die ordnungsgemäße Wartung eines Giftstofftanks unterlassen; der Giftstofftank lief über. Der Mitarbeiter hatte sich auf die nachgeschalteten Sicherheits- bzw. Auffangbecken verlassen. Das Bundesgericht stellte klar, dass man sich nicht auf Mehrfachsicherungssysteme verlassen dürfe. Es reiche vielmehr für die Strafbarkeit nach Geschäftsherrenhaftungsregeln, wenn man für den inkriminierten Erfolg lediglich eine Teilursache setze. Auch vor dem Hintergrund dieses Bundesgerichtsentscheides wird klar, dass man sich nicht leichtthin auf Sicherheitsvorkehrungen anderer, wie sie z.B. mittels einer Konformitätsprüfung (CE-Kennzeichen) bestätigt werden, verlassen darf. Man kommt im Rahmen der Produktesicherheits-Compliance (ja überhaupt in der Compliance) um die eigenen Sorgfaltspflichten nicht herum.

17

Im „Zisternen-Fall“ (BGer 6S.447/2003) war eine mehrere Tonnen schwere Zisterne auf einem untauglich konstruierten Rollbock montiert. Es kam zum Kippen der Zisterne in Richtung einer anderen Zisterne, an der ein Arbeiter gerade hantierte, und in der Folge zum tödlichen Unfall. Der für die Arbeitersicherheit Bereichsverantwortliche wurde wegen fahrlässiger Tötung verurteilt, weil er die Sicherheitsrisiken nicht evaluiert hatte, kein Sicherheitskonzept existierte und keine Schutzmaßnahmen einschließlic adäquater Information der Mitarbeitenden über die Gefahren und einer Anleitung über Verhütungsmaßnahmen vorhanden waren. Das Bundesgericht stellte auch klar, dass der Sicherheitsverantwortliche nicht auf das ordnungsgemäße Bedienen des Geräts vertrauen dürfe, und dass ihn eine Pflicht zur Mehrfachsicherung des Geräts treffe. Dies gelte selbst dann, wenn ihm keine unmittelbare Tatmacht zukomme; alsdann müsse er eben solche Mehrfachsicherungen, Sicherheitsrisikoevaluationen und die Entwicklung von Sicherheitskonzepten etc. bei seinem Vorgesetzten beantragen. Fazit: Das Weisungswesen muss Mehrfachsicherungen gefahrengeneigter Produkte sowie Meldekanäle zwecks Mitteilung und Behebung vermuteter Sicherheitslücken vorsehen.

18