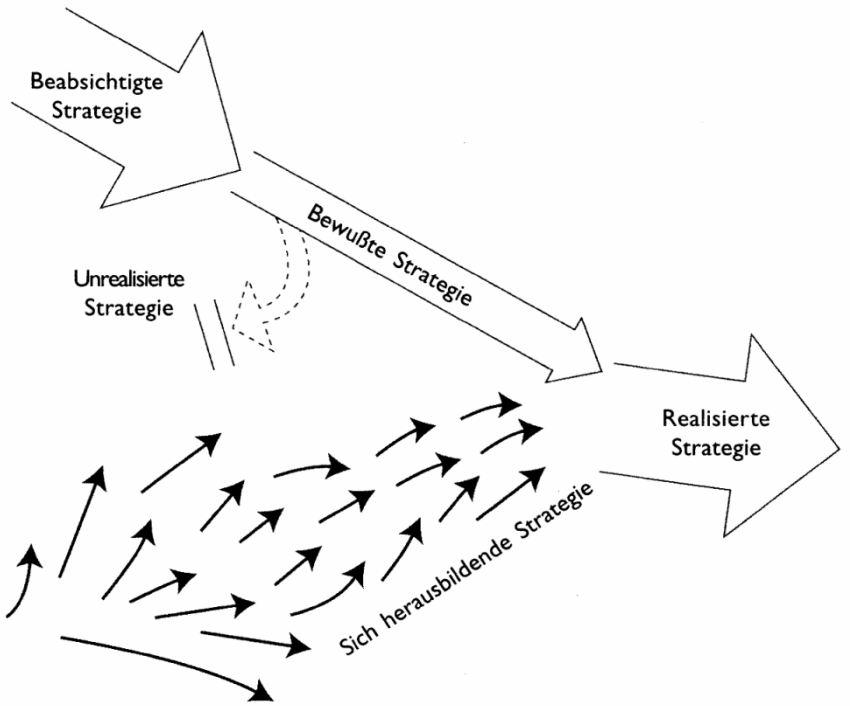
# Möglichkeiten und Grenzen des Information Security Management

Ein Experte ist jemand, der die Schwächen seines Systems kennt.

Der Begriff »*Emergenz*« lässt sich etymologisch vom lateinischen emergo ableiten, das übersetzt »auftauchen, sich zeigen« bedeutet. So interpretiert eine im Managementkontext populäre Sicht von Mintzberg Emergenz als die nicht explizit beabsichtigten, »sich herausbildenden« Ergebnisse einer Strategie (s. Mintzberg/Ahlstrand/Lampel 1999, S. 26):




Kahle fasst Emergenz allgemein als »Strukturentwicklung auf der Basis einfacher Regeln« auf (s. Kahle 1995, S. 24).

Als gemeinsamer Nenner der meisten Emergenz-Interpretationen kann eine Informationsasymmetrie unterstellt werden: Würde Emergenz nur als Ergebnis eines Systemverhaltens interpretiert, also ohne besondere Berücksichtigung eines Komplexitätsgefälles, wäre das Konzept trivial (Kahle spricht beispielsweise explizit von »einfachen« Regeln).

Emergenz als Komplexitätsgefälle zu Lasten eines Beobachters ist demnach ein Desinformationsphänomen, das sich aus unterschiedlichen Perspektiven behandeln lässt. Als unabhängige und somit frei kombinierbare Leitunterscheidungen bieten sich hier beispielsweise an:

- eine statische versus dynamische Betrachtung
- eine ex ante- versus ex post-Analyse

- eine aktive versus passive Perspektive.

Bei der statischen Sicht werden Systemzustände, bei der dynamischen Systemverhalten miteinander verglichen.
Die ex ante Perspektive entspricht der Prognose eines Beobachters, bei der ex post-Betrachtung erfolgt ein nachträglicher Vergleich.
Der aktive Zugang betont die Gestaltung eines Systems, während der passive sich mit der Betrachtung selbst begnügt.

Weiterhin lässt sich danach unterscheiden, ob »echte« oder »Pseudo-«Emergenz vorliegt: so differenziert etwa die Komplexitätstheorie nach deterministischem und nichtdeterministischem Chaos. Im ersten Fall lässt sich ein Systemverhalten grundsätzlich mit Sicherheit prognostizieren, was im nichtdeterministischen Fall per definitionem nicht möglich ist.[1]
»Unechte« Emergenz wird häufig aus Wirtschaftlichkeitserwägungen in Kauf genommen.[2]
Zudem ist Emergenz ein kybernetischer Begriff höherer Ordnung, der auf sich selbst angewandt werden kann, was auch »Emergenzen von Emergenzen« ermöglicht.
Aus der Wissensqualitätsperspektive ist letztlich entscheidend, ob qualitative Desinformation vorliegt oder nicht (vgl. Glück 2002).

In allen Fällen gilt, dass die Informationsasymmetrie bzw. das Komplexitätsgefälle beobachterabhängig ist. Was einem Betrachter als emergent erscheint, muss es nicht zwingend auch für einen anderen sein.
Außerdem gerät nicht alles, was emergiert, zur emergency: auch die Bewertung von Emergenz hängt von der jeweiligen Interessenslage ab und liegt somit im Auge des Betrachters.
Nicht zuletzt stellt Emergenz angesichts allgegenwärtiger Komplexitätsdifferenzen weniger eine Ausnahme als die Regel dar.[3] Ashby forderte demgemäß in seinem kybernetischen »Grundgesetz« die Herstellung korrespondierender Komplexitäten.[4]

*Steuerung* kann generell als Gestaltung von Systemverhalten aufgefasst werden. Abgesehen von trivial-deterministischen Systemen lässt sie sich auch als Management von Komplexitätsdifferenzen oder als »Nichtwissens-Management« interpretieren.

Bei Übertragung dieser Sichtweise auf die Steuerung von Organisationen und unter der Annahme, dass die Komplexität der Organisation grundsätzlich größer ist als die der Steuerung, gibt es zwei Zielrichtungen für die Herstellung korrespondierender Komplexität: Erhöhung der Komplexität der Steuerung oder Komplexitätsreduktion der zu steuernden Organisation.

---

[1] Als Analogie bietet sich hier der Vergleich zwischen echten und Pseudo-Zufallszahlen an. So kann etwa eine Verschlüsselungstechnologie, die keine stochastisch unabhängigen Zufallsfolgen liefert, grundsätzlich gebrochen werden.
[2] Als Beispiel kann die Anwendung einer Heuristik auf ein Problem dienen, das sich auch algorithmisch lösen ließe.
[3] Für eine Diskussion von Komplexität im Kontext organisationaler Intelligenz vgl. Glück 2002, S. 203 ff.
[4] Er nannte sein Gesetz »law of requisite variety« vgl. Ashby 1971, S. 206 ff.. Varietät ist aus informationstheoretischer Perspektive ein Komplexitätsmaß für die Mächtigkeit einer Elementarereignismenge.

Letzteres ist umso problematischer, je mehr Beziehungen zur organisationalen Umwelt bestehen. Die Organisation selbst ist unter Umständen nicht mehr in der Lage, adäquat auf veränderte Umweltbedingungen zu reagieren und wird ggf. sogar in ihrem Bestand gefährdet, falls die falschen Komplexitäten reduziert wurden. Steuerung kann also – ebenso wie Emergenz – je nach Kontext nützlich oder schädlich sein (vgl. Glück, Wirksamkeit, 2005).

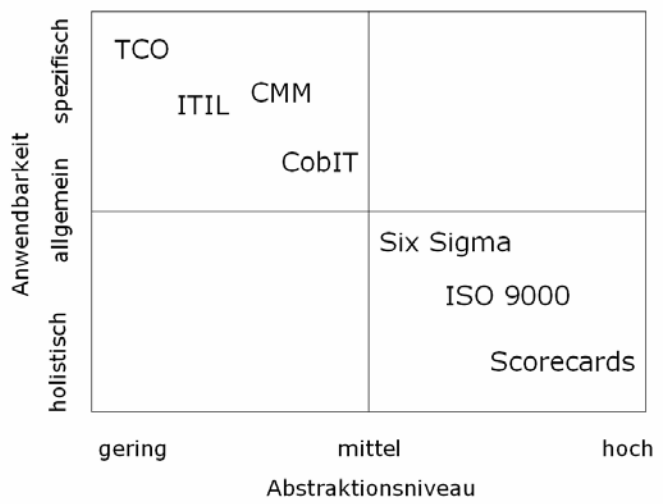
Die Prämisse »adäquaten« Reagierens zeigt, dass auch der Komplexitätsbegriff alleine noch keine bewertenden Aussagen zulässt. Eine Interpretation der Komplexität als quantitatives Maß für Ereignisse macht noch nicht notwendigerweise Aussagen zur Konstruktion des Ereignissystems und insbesondere zum Zielsystem als Bewertungsgrundlage. Ein Kreuzen von Komplexitäts- mit Rationalitätsaspekten ermöglicht diesbezügliche konzeptionelle Erweiterungen (vgl. Glück 2002, S. 203 ff.).

Als »Werkzeuge« zur Organisationsgestaltung dienen *Strukturationen*. Die Bandbreite reicht von interpretationsbedürftigen Taxonomien zur Sprachregelung über Verfahrens- und Handlungsanweisungen bis hin zu Regelsystemen, welche Bewertungsprozesse steuern.
Eine langjährige internationale Studie der Unternehmensberatung Bain & Company zählt beispielsweise zu den in 2007 populärsten Tools:[5]

- Balanced Scorecard
- Benchmarking
- Business Process Reengineering
- Core Competencies
- Customer Relationship Mgmt.
- Customer Segmentation
- Growth Strategy Tools
- Knowledge Management
- Mission and Vision Statements
- Offshoring
- Outsourcing
- Scenario and Contingency Planning
- Shared Service Centers
- Six Sigma
- Strategic Alliances
- Strategic Planning
- Supply Chain Management

Die folgende Graphik zeigt eine beispielhafte Verortung insbesondere von mehr oder weniger standardisierten Qualitäts- und Prozessmanagementstrukturationen (Gartner zit. v. Anthes 2004):[6]

[5] in alphabetischer Reihenfolge, vgl. Rigby/Bilodeau 2007.
[6] TCO: total cost of ownership; ITIL: IT Infrastructure Library; CMM: Capability Maturity Model; CobIT: Control Objectives for Information and Related Technology.




Besonders interessant erscheint, dass Gartner die Anwendbarkeitsskala bei »holistisch« beginnen lässt. Tatsächlich kann aber auch der „ganzheitlichste" Ansatz nur das enthalten, was man bei seiner Anwendung damit assoziiert (das Akronym GIGO charakterisiert den Zusammenhang zutreffend: garbage in, garbage out).
Die beste Annäherung an einen ganzheitlichen Zugang bieten generische Ansätze, die zur Erfüllung dieses Anspruches aber eben auch entsprechend appliziert werden müssen.[7]

Das Management hat die Auswahl aus einer kaum überschaubaren Vielzahl von nicht zwingend überschneidungsfreien, mitunter ineinander verschachtelten Strukturationen. Ihre unkritische Anwendung birgt nicht geringe Risiken: Nicht alles, was im Rahmen »standardisierter« Prozesse erhebbar ist und erhoben wird, ist auch erheblich, woraus zumindest Opportunitätskosten erwachsen.
Die Ignoranz des Komplexitätsgefälles zwischen Strukturation und zu steuerndem Sachverhalt verkehrt das Steuerungsziel nicht selten in sein Gegenteil.[8] Kontrollillusion mündet in Kontrollverlust, die Anmaßung von Dynamik in zunächst statischen Modellen neigt zur Entstehung von Kernrigiditäten und Bürokratismen: die Organisation emergiert zum Feind der Organisation (vgl. Glück, Kompetenz, 2005).

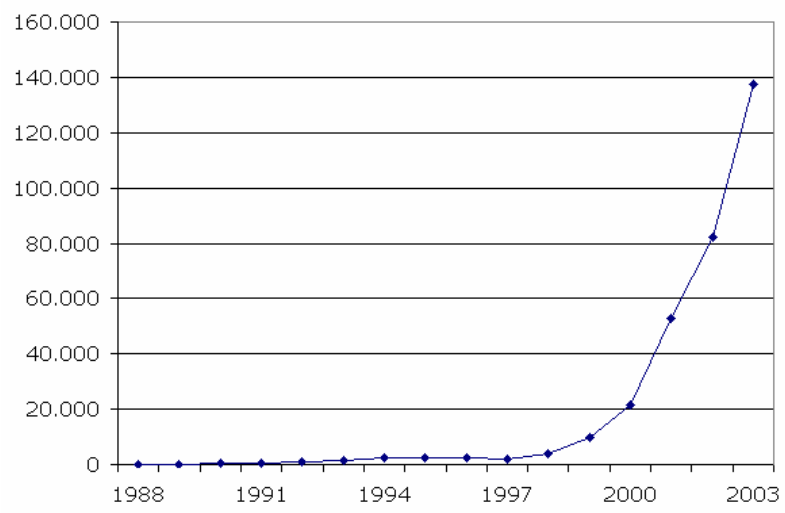
Die aus der unintelligenten Anwendung von Strukturationen resultierenden Risiken korrespondieren mit den Chancen der Wettbewerber. Bereits um 500 v. Chr. betonte Sun Tsu die ökonomische Bedeutung von Informationsvorsprüngen in der Strategie. Nicht zuletzt mit zunehmender Wissensintensität der Organisation steigt auch die Relevanz von Informationsasymmetrien.[9]

---

[7] Einer der ersten generischen Ansätze wurde von Ramon Llull (1232-1316) in der Ars Magna entwickelt, als deren Urenkel Kahles Helidem interpretiert werden kann (vgl. Kahle/Wilms 1998).
[8] Dies gilt insbesondere bei passiver Desinfomation bezüglich des Instrumentariums, vgl. Glück 2002 S. 107 ff.
[9] Sun Tsu schreibt: »Der Grund, warum kluge Herrscher und gute Heerführer den Feind schlagen, wo auch immer er sein mag, und warum ihre Leistungen die Taten gewöhnlicher Menschen übersteigen, ist das Vorauswissen. […] Was man als Vorauswissen bezeichnet, kann man weder von Geistern noch von Göttern erfahren, weder durch Vergleiche mit vergangenen Begebenheiten, noch durch Berechnungen. Man muß es von den Leuten erfahren, die die Feindlage gut kennen« (vgl. Sun Tsu 1989, S. 91).

Vor dem Hintergrund der Emergenzdiskussion ist kaum ein Gebiet komplexer und dynamischer als das Informationssicherheitsmanagement. Es stellt insofern höchste Anforderungen an eine intelligente Organisationsgestaltung.

Der folgende Graph zeigt beispielsweise, dass die international gemeldeten Sicherheitsvorfälle im Internet bis 2003 exponentiell zunahmen (Quelle: CERT):




Die Erfassung endete in 2003, weil ihre Aussagekraft angesichts der weiten Verbreitung automatisierter Angriffswerkzeuge nur noch als gering eingeschätzt wurde. Zudem veränderte sich der Angreiferfokus: Während es in den Anfangsjahren als Frage der Ehre galt, möglichst öffentlichkeitswirksam auf sich aufmerksam zu machen, legen Geheimdienste und die mehr oder weniger organisierte Kriminalität Wert darauf, im Verborgenen zu wirken (vgl. Kossel/Kötter 2007).

Im »information warfare« stellt das Internet nur eines von vielen Schlachtfeldern dar. Organisationen können – unabhängig von ihrer Wissensintensität – mit ihrer Informations- bzw. Wissensbasis identifiziert werden, wodurch sich grundsätzlich Angriffspunkte in allen organisationalen Bereichen ergeben (vgl. Glück 2002, S. 5).
Eine umfassende Studie unter Federführung von Egbert Kahle liefert zahlreiche Fallstudien über entsprechende Schadenfälle in Baden-Württemberg und ermöglichte erstmals eine empirisch abgesicherte Hochrechnung für das Gefährdungspotential, das sich deutschlandweit mit ca. 50 Mrd. EUR p.a. beziffern lässt (vgl. Kahle/Merkel 1995, S. 61). Dabei flossen in diese Kalkulation nur direkte Schäden ein; nicht zu unterschätzen sind beispielsweise Reputations- und Markenschäden im internationalen Umfeld durch i.d.R. minderwertigere Plagiate.
Demgegenüber konnten die Aufwendungen für Informationssicherheitsmaßnahmen als sehr gering bezeichnet werden (vgl. Kahle/Merkel 1995, S. 63). Kahle empfiehlt zur Prävention (vgl. Kahle/Merkel 1995, S. 72 ff.):

1. Die Erstellung von Informationsschutzkonzepten, welche personelle, organisatorische, technisch/-bauliche sowie rechtliche Maßnahmen umfassen sollten.[10]
2. Die Entwicklung einer Wissensbilanz bzw. eines Informationsinventars
3. Die Entwicklung eines dynamischen Risikomanagementkonzeptes
4. Die Entwicklung von interdisziplinären Schulungsmaßnahmen zum Themenkomplex Sicherheitsmanagement.[11]

Informationssicherheitsmanagement verfolgt allgemein folgende Schutzziele:

- *Vertraulichkeit*: Informationen dürfen Unbefugten nicht zugänglich gemacht werden.
- *Integrität*: Informationen sind vor unbefugter Veränderung zu schützen
- *Verfügbarkeit*: Informationen müssen im Bedarfsfall zugänglich sein
- *Nachvollziehbarkeit*: Informationen müssen ihrer Quelle zuordenbar sein.

Verletzungen dieser Schutzziele können beispielsweise von höherer Gewalt ausgehen (etwa durch Naturkatastrophen), auf organisationalen Mängeln oder menschlichen Fehlhandlungen, auf technischem Versagen oder eben auf vorsätzlichem Handeln basieren.

Was das Problemfeld besonders anspruchsvoll macht, ist die Tatsache, dass die für einen potentiell Gefährdeten empfindlichsten Schwachstellen von ihm selbst nicht wahrgenommen werden. Würde man die Schwächen sehen, dann könnte man entsprechende Maßnahmen ergreifen, sofern man es für nötig erachtet. Dies gilt freilich generell im strategischen Kontext: »Knowing a competitor's blind spots […] will help […] to identify competitor weaknesses.« (Zajac/Bazermann 1991, S. 39)[12]

Aus demselben Grund ist eine quantifizierte Risikobewertung oftmals schwierig bis unsinnig. Die Problematik liegt darin, geeignete Ereignissysteme mit (je nach Szenario sehr subjektiven) Eintrittswahrscheinlichkeiten zu definieren: man bewegt sich häufig in einem Bereich von Entscheidungen unter Unsicherheit im engeren Sinn.[13] Nur ein Teil der Informationssicherheitsrisiken ist überhaupt quantifizierbar (und dieser Teil sollte, nachdem die Schwachstellen dort mit Eintritt des Schadens normalerweise[14]

[10] für einen entscheidungstheoretischen Rahmen für das Security-Management aus personalwirtschaftlicher und organisatorischer Perspektive vgl. Kahle 2002.

[11] als Pilotprojekt kann hier der berufsbegleitende Weiterbildungsstudiengang Strategisches Management mit dem Schwerpunkt Security Management am Zentrum für Wissenschaftliche Weiterbildung der Universität Lüneburg genannt werden. Für ein konzeptionelles Grundlagendokument in diesem Kontext s. Kahle 2002.

[12] Für einen umfassenden Überblick zur »Blinden-Fleck-Forschung« und die Einführung qualitativer blinder Flecken als organisationale Basisrestriktion siehe Glück 2002.

[13] Ein hypothetisches Beispiel: Ein System, das der Verwaltung von Textbausteinen für die Vertragsgestaltung dient, weist eine Schwachstelle auf, wodurch für das Unternehmen ungünstige Verträge erstellt und rechtswirksam werden könnten. Mit welcher Höhe soll man die potentiell resultierenden Schäden ansetzen? Welche Eintrittswahrscheinlichkeiten sollte man den jeweiligen Schadenszenarien zuordnen? Weitere Beispiele sind die Beurteilung eines Imageschadens oder eine Szenarienanalyse zur Einschätzung eines Geschäftsverlustes durch „nicht realisierte Vertragsabschlüsse".

[14] Für Kahle ist eine »Bewusstmachung des Problems der Informationsgefährdung […] besonders bedeutsam, weil aus Gründen des „Gesichtsverlusts", aber auch der inneren Betroffenheit von solchen Informationsverletzungen, die davon Betroffenen nicht darüber reden und damit die Öffentlichkeit oder

auch bekannt wurde, zumindest am Schadensort nicht lange bestehen bleiben). Es ist eine Plattitüde, dass eine Kette nur so stark wie ihr schwächstes Glied sein kann. Hier kommt erschwerend hinzu, dass die Kette womöglich den falschen Zugang schützt.

Unter Berücksichtigung der vorgenannten Restriktionen und vor dem Hintergrund der Emergenzproblematik lassen sich einige Designempfehlungen für die Realisation eines intelligenten, wirksamen Information Security Management Systems (ISMS) aussprechen.[15] Zielsetzung ist die Minimierung von Prozesskosten und Durchlaufzeiten bei maximaler Ergebnisqualität, was ein evolutionäres, anpassungsfähiges Grundkonzept bei redundanzfreier Integration aller abhängigen Prozesse voraussetzt.

Als Ausgangspunkt bieten sich diverse Strukturationen an. International am prominentesten sind die Standards der International Organization for Standardization (ISO) und der International Electrotechnical Commission (IEC). Sie lassen sich auf best practises zurückführen, die zunächst vom British Standards Institute im BS 7799-1:1995 formuliert wurden. Er gilt als erster »offizieller« Standard im Informationssicherheitskontext. In der Version BS7799-1:1999 wurde er von der ISO als ISO/IEC 17799:2000 übernommen. Die aktuelle Revision trägt den Namen ISO/IEC 27002 und ist Teil der ISO/IEC 27000-Standardserie.
Wesentlicher Bestandteil von Informationssicherheitsmanagementstrukturationen ist ein Regelwerk als Basis für Prüfungen und Bewertungen: Abweichungen vom Regelwerk sind prinzipiell als Sicherheitslücken zu interpretieren.

Das Regelwerk ist als Prüf- und Bewertungsbasis der Dreh- und Angelpunkt der Securitymanagementprozesse. Eine initiale Version ergibt sich gewöhnlich aus der für die Sicherheitsorganisation zugrundegelegten Strukturation. Nicht erfüllte Regeln sollen als Schwachstellen gelten.
Falls bekannte Bedrohungen existieren, die noch nicht durch das Regelwerk adressiert werden, so ist das Regelwerk enstprechend anzupassen bzw. zu erweitern. Eine darüber hinausgehende Entwicklung von Bedrohungskasuistiken und Taxonomien empfiehlt sich nicht: Während die Suche nach potentiellen Bedrohungen sowie deren Zuordnung von Schutzzielen einerseits kontextabhängig und damit erklärungsbedürftig ist, ist andererseits eine Vollständigkeit der Analyse nicht gewährleistet (abgesehen von trivialen, entsprechend konstruierten Beispielfällen). Ein handfester Nutzen würde sich dann ergeben, wenn sich konsistente, »vollständige« Ereignissysteme mit Eintrittswahrscheinlichkeiten von der Bedrohung bis hin zum potentiell realisierten Schaden konstruieren ließen, um auf dieser Basis Schadenserwartungswerte zu berechnen. Dies wird in der Praxis nur in sehr wenigen, speziellen Fällen möglich sein. In allen anderen gilt: es ist besser, ungefähr richtig zu liegen, als präzise falsch.

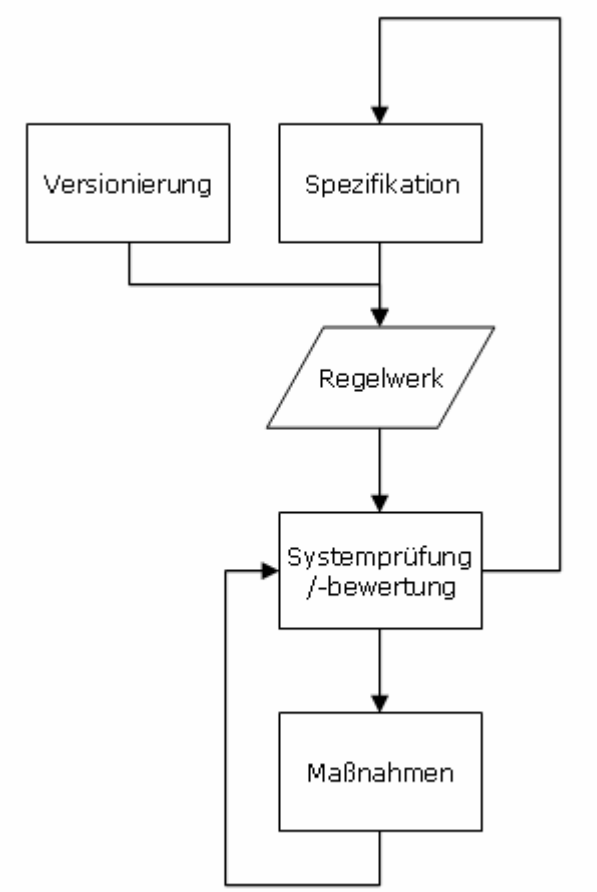
Das basale Regelwerk dürfte zunächst ebenso abstrakt wie umfangreich sein, was seine unmittelbare Anwendbarkeit beeinträchtigt. Nicht jede Regel ist für jeden organisationalen Kontext einschlägig, nicht jede tatsächlich anzuwendende Regel ist für

---

die relevanten „Mitbetroffenen“ - weil zukünftig Gefährdeten - nichts davon erfahren« (Kahle/Merkel 1995, S. 1)

[15] Die genannten Aspekte wurden vom Autor bei der Konzeption und Implementierung des Information Security Management Systems eines internationalen Finanzdienstleistungskonzerns erfolgreich umgesetzt.

den Anwender verständlich. Je nach Situation sind einzelne Regeln womöglich unterschiedlich zu interpretieren. Um hier eine »Paralyse durch Analyse« zu vermeiden, ist eine situative Spezifikationsmöglichkeit vorzusehen, die auch entscheidungsunterstützende Kontextinformationen für die individuellen Prüf- und Bewertungsprozesse bietet.
Die folgende Abbildung gibt einen grundlegenden Überblick zu den erörterten Aspekten:




Der Begriff »System« ist hier maßstabsunabhängig zu verstehen und kann die gesamte Organisation, Teile daraus oder Prozesse umfassen. Ebenso ist das ISMS selbst skaleninvariant und generisch zu realisieren, um sich Veränderungen der Systemlandschaft flexibel anpassen zu können. Eine angemessene Rollengestaltung bei entsprechender Prozessverteilung lässt unnötige administrative Zwischenschichten obsolet werden.
Durch die Integration von heterarchischen und hierarchischen Organisationsprinzipien kann Ashby's Anforderung korrespondierender Komplexität entsprochen werden.

Sofern Prüfungen Sicherheitslücken aufzeigen, sind diese mit geeigneten Maßnahmen zu behandeln. Aus dem Prüfkontext können sich wiederum Spezifikationsanpassungen ergeben.
Die Prüfungs- und Bewertungsergebnisse sollen sich in Echtzeit zu Compliancereports auf beliebigem Aggregationsniveau und aus verschiedenen Perspektiven konsolidieren

lassen. Dabei ist auf Robustheit bzgl. unscharfer und fehlender Informationen zu achten (etwa durch die Berücksichtigung entsprechender Signifikanzmaße).

Der Betrieb des so konzipierten Information Security Management Systems führt zu einer laufenden Inventarisierung der Organisation aus unterschiedlichen Blickwinkeln, woraus nicht zuletzt Synergien in Form von verbesserten Steuerungspotentialen für die Unternehmensführung resultieren.

Die wiederholte Anwendung einfacher, generischer Konzepte muss nicht nur Emergentes entstehen lassen – man kann auch komplexe Systeme damit steuern.

Zitierte Quellen:

Anthes, G.: Quality Model Mania, Computerworld, 08.03.2004

Ashby, W. R.: An introduction to cybernetics, London: Chapman & Hall, 1971

Glück, T. R.: Blinde Flecken in der Unternehmensführung : Desinformation und Wissensqualität, Passau: Antea, 2002

Glück, T. R.: Kultur und Kompetenz, Passau: Antea, 2005

Glück, T. R.: Wirkung und Wirksamkeit, Passau: Antea, 2005

Kahle, E.: Entscheidungs- und organisationstheoretische Grundlagen des Security Managements in Unternehmen, Wissenschaftlicher Arbeitsbericht des ZWW, Lüneburg, 2002

Kahle, E.: Kognitionswissenschaftliche Grundlagen von Selbstorganisation, Arbeitsbericht 01/95 der Forschungsgruppe kybernetische Unternehmensstrategie (FOKUS), Universität Lüneburg, 1995

Kahle, E.: Security-Management unter HR- und Organisationsaspekten, in Personalführung 5/2002

Kahle, E.; Merkel, W.: Fall- und Schadensanalyse bezüglich Know-how-/Informationsverlusten in Baden-Württemberg ab 1995, Schlussgutachten Stand 10.06.2004, Universität Lüneburg

Kahle, E.; Wilms, F. E. P.: Der Helidem : Eine nichthierarchische Form der Analyse komplexer Wirkungsbeziehungen, Aachen: Shaker, 1998

Kossel, A.; Kötter, M.: Piraten-Software, in c't special 03/2007 - Security, Heise

Mintzberg, H.; Ahlstrand, B.; Lampel, J.: Strategy Safari, Wien: Ueberreuter, 1999

Rigby, D.; Bilodeau, B.: Management Tools and Trends 2007, Bain & Company, 2007, http://www.bain.com/

Sun Tsu: Über die Kriegs-Kunst, übers. u. kommentiert v. Leibnitz, K., Karlsruhe: Info Verlagsgesellschaft, 1989

Zajac, E.J.; Bazermann, M.H.,: Blind Spots in industry and competitor analysis, in: Academy of Management Review, Vol. 16, No. 1, 1991