

# Von Böcken und Gärtnern - zur Rolle der IT in der Corporate Governance und Compliance





- Ein kurzer Blick auf Governance und Compliance
- Die IT als Problemverursacher
- Die IT als Lösungskomponente
- Governance-/Compliance-Regeln für die IT
- Aktueller Stand und Trends

# Ein kurzer Blick auf Governance und Compliance



# Compliance und Governance

- **Compliance** (*Befolgung*): Einhaltung von Verhaltensmassregeln, Gesetzen und Richtlinien in Unternehmen
- IT Compliance: regelkonformer Einsatz der IT sowie Einsatz der IT zur Überwachung
- **Governance**: „gutes“, d. h. gesellschaftlich verantwortliches und faires Management über Verhaltenskodices (Leitlinien) fördern
- IT-Governance: Führung, Organisationsstrukturen und Prozesse, die sicherstellen, dass die IT die Unternehmensstrategie und -ziele unterstützt

# HaL's „3 goldene Regeln“ der Compliance

- Tun Sie das Richtige → Gesetze und Regulation  
(Fehlverhalten kann zu Strafverfolgung führen)
- Tun Sie es richtig → “best practices”, IKS, etc.  
(Fehlverhalten kann viel Geld kosten)
- Seien Sie in der Lage, jederzeit zu beweisen, dass Sie  
das Richtige richtig getan haben → Compliance  
(Fehlverhalten kann zum Verlust der Lizenz, von  
Marktanteilen, Glaubwürdigkeit, Umsatz, Kunden,  
Partner, Mitarbeitenden, Lieferanten etc. führen)



# Quis custodit custodes?

[Juvenal]

- Mangelhaft spezifizierte und implementierte Zugriffsrechte, dadurch kaum nachvollziehbare Veränderungen
- Mangelhafte Gewaltentrennung in Software und Betrieb
- Zu hohe Privilegien der Systembetreuer
- Schwer kontrollierbare negative Effekte der wachsenden Vernetzung
- Fähigkeit zur unkontrollierten Datensammlung, Auswertung und verlustfreien, unautorisierten Weitergabe
- Sprunghafter Komplexitätszuwachs
- Intransparenz der angebotenen / betriebenen Lösungen
- Abhängigkeiten von geschäftskritischen Infrastrukturen

Chronology of Data Breaches Go to Breaches for <a href="#">2005</a> , <a href="#">2006</a> , <a href="#">2007</a> , <a href="#">2008</a> or <a href="#">2009</a>			
DATE MADE PUBLIC	NAME(Location)	TYPE OF BREACH	NUMBER OF RECORDS
Oct. 27, 2009	FirstMerit Bank (Streetsboro, Westlake and Elyria, OH)	Police in three Ohio cities are investigating the theft of three large storage bins from bank branches earlier this month. The storage bins were used to store paper waiting to be shredded. Three branches of the FirstMerit Bank in Streetsboro, Westlake and Elyria, OH each reported a bin missing beginning on October 7. One of the three bins contained personal documents of bank customers.	Unknown
Oct. 28, 2009	Llywelyn's Pub (Overland Park, KS)	Llywelyn's Pub and its customers are the victims of a sophisticated cyber credit card attack. The crimes were the result of a hacker, who managed to gain access to the information between the time of sale and the point at which the information reached the credit card processing company. The credit card information has been used illegally in various states, but mostly southern states.	Unknown
Oct. 28, 2009	New York Mellon Corp. (New York, NY)	A computer technician has been charged with allegedly stealing the identities of more than 150 Bank of New York Mellon Corp. employees and using their identities to steal more than \$1.1 million from charities, non-profit groups and others. The man was employed by a contractor that did work for Bank of New York, was charged in a 149-count indictment. The man was arrested in April when the U.S. Secret Service executed a search warrant on his home and found Bank of New York employees' credit reports on his computer, along with many other documents containing personal identifying information of more than 150 Bank of New York employees.	150
TOTAL number of records containing sensitive personal information involved in security breaches in the U.S. since January 2005.			340,097,773 <a href="#">What does the total number indicate?</a>
Printing tip: Use the "landscape" setting for best results when printing the breach list.			

<http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP>

[ABOUT](#) | [DISCLAIMERS](#) | [ARCHIVES](#) | [TWITTER](#) | [BLOG ROLL](#)

## The Rise in Financial Crime in America

Posted on Tuesday, July 21st, 2009 at 12:15 pm.

[The Economist is reporting](#) that there were over 730,000 counts of suspected financial wrongdoing recorded in America last year. Financial institutions filed nearly 13% more reports of fraud compared with 2007. The number of mortgage frauds rose by 23% to almost 65,000.

This poses the classic compliance conundrum: Is there more fraud occurring, *or* is more fraud being detected/reported?

Source: US Financial Crimes Enforcement Network

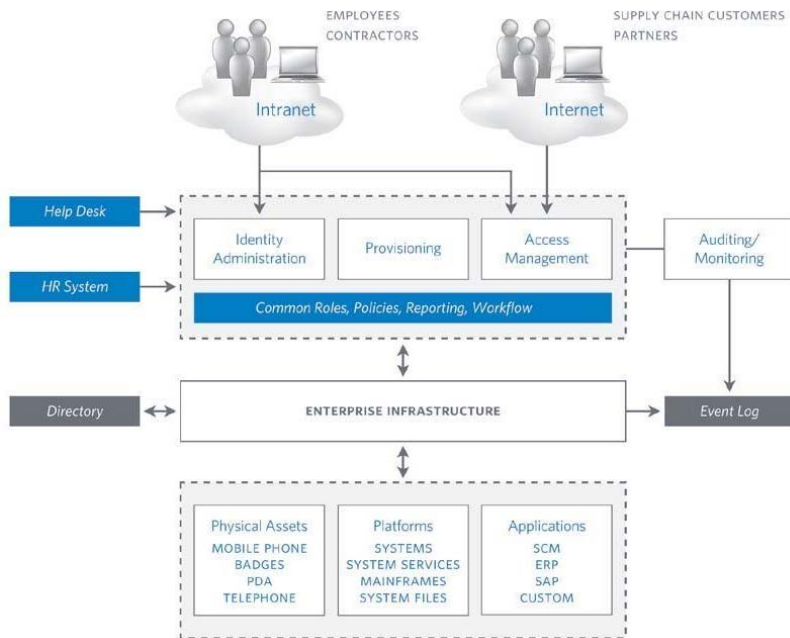
<http://www.compliancebuilding.com/2009/07/21/the-rise-in-financial-crime-in-america>



# Die IT löst Probleme, die ohne sie nie entstanden wären ...

---

- Implementation genügend starker Zugriffsregeln und eines Mehraugenprinzips
- Automatisierte Forcierung der Umsetzung / Einhaltung
- Anlage, Sammlung und systematische Auswertung von Ereignisprotokollen
- Echtzeit-Überwachung, Alarmierung und Eskalation bei Unregelmässigkeiten



[http://www.monitor.co.at/ausgaben/2008\\_03/ca\\_iam~fs.jpg](http://www.monitor.co.at/ausgaben/2008_03/ca_iam~fs.jpg)

[http://www.gbtec.de/app/webroot/img/Image/screenshots\\_big/screen22.jpg](http://www.gbtec.de/app/webroot/img/Image/screenshots_big/screen22.jpg)

# Governance-/Compliance-Regeln für die IT



1. Wissen was man hat (ICT, Personal, ... → IT Asset Mgmt)
2. Wissen wer wer ist (Identity Mgmt)
3. Wissen wer was darf (Provisioning, Rollen, Rechte)
4. Wissen wer was tut (Access Control & Logging)
5. Wissen welche Bedrohungen relevant sind- diese Bedrohungen erkennen und abwehren (Threat Mgmt)
6. Den IT – Bebauungsplan definieren & kennen (Architektur)
7. Den Gesamtüberblick haben (C & C, SIEM)
8. Handlungen ableiten (Trouble Ticketing, Alarmierung, Eskalation)
9. Den Life Cycle bewirtschaften
10. Alle Veränderungen überwachen (inkl. Backup/Archiv)
11. Ausweichinfrastrukturen für den Krisenfall bereitstellen
12. Tätigkeits- und Beweisprotokollierung sicherstellen

1. Klare Zuordnung und Umsetzung von Auftrag, Rollen, Verantwortlichkeiten und Kompetenzen
2. Definition und Pflege der organisatorischen und Prozessbedingten Schnittstellen
3. Festlegung des zu erreichenden Wunschzustandes und Festlegung der Messgrößen und Massnahmen
4. Sofortmassnahmen definieren und umsetzen
5. Vollständige und jederzeit aktuelle Dokumentation
6. Kontinuierlichen Verbesserungsprozess etablieren
7. Regelmässige Bewertung des Status als nicht delegierbare Management-Aufgabe
8. Regelmässiges Reporting zur Geschäftsleitung
9. Systematische Auswertung von Schadenfällen und „near misses“
10. Bewusstsein für die Problematik fördern, ggf. in die Personalbewertung integrieren



# Aktueller Stand und Trends

- Konstante(?) Anzahl von IT-induzierten Sicherheitsmängeln
- Zu hohe Komplexität mit kaum gebremstem Wachstum (Software, Prozesse, ...)
- Stetig längere, verteilte Wertschöpfungs- und Abhängigkeitsketten
- Zunehmend komplexe und zeitverzögerte Rechts- und Regulationslage (bes. in multinationalen Umgebungen)
- Wachsender Einfluss der Auslagerung von IT-Leistungen als Teil der Reduktion der betrieblichen (Fix)-Kosten
- Hohe Sensitivität der diversen „stake holder“ für Themen der Governance und Compliance



- Mängel an komplexen IT-Systemen haben in der Vergangenheit nicht selten zu Schwachstellen, Verstößen gegen Compliance-Richtlinien und zur Schwächung der Corporate Governance geführt.
- Andererseits ist eine sowohl effektive als auch effiziente Umsetzung von Compliance- und Governance-Anforderungen ohne IT-Systeme kaum denkbar.
- In diesem Spannungsfeld muss die IT einen schwierigen Spagat zwischen Problem-Verursacher und Problemlöser meistern.

# Manchmal funktionieren Böcke als Gärtner doch



# Besten Dank für Ihre Aufmerksamkeit

---

Fachhochschule Nordwestschweiz  
Hochschule für Technik  
Institut für Mobile und Verteilte Systeme

Prof. Dr. Hannes P. Lubich  
Dozent für ICT System Management  
Steinackerstrasse 5, CH-5210 Windisch

T: +41 56 462 4758 (direkt)  
hannes.lubich@fhnw.ch

[www.fhnw.ch](http://www.fhnw.ch)