it.sec
security for your information

GRC Erfahrungen mit dem Tool Risk Vision in einem Bankprojekt

Holger Heimann/it.sec

GI Fachgruppe Management von Informationssicherheit
Frankfurt am Main, 11.6.2010

Dipl. Ing (FH) Holger Heimann

(CISA)

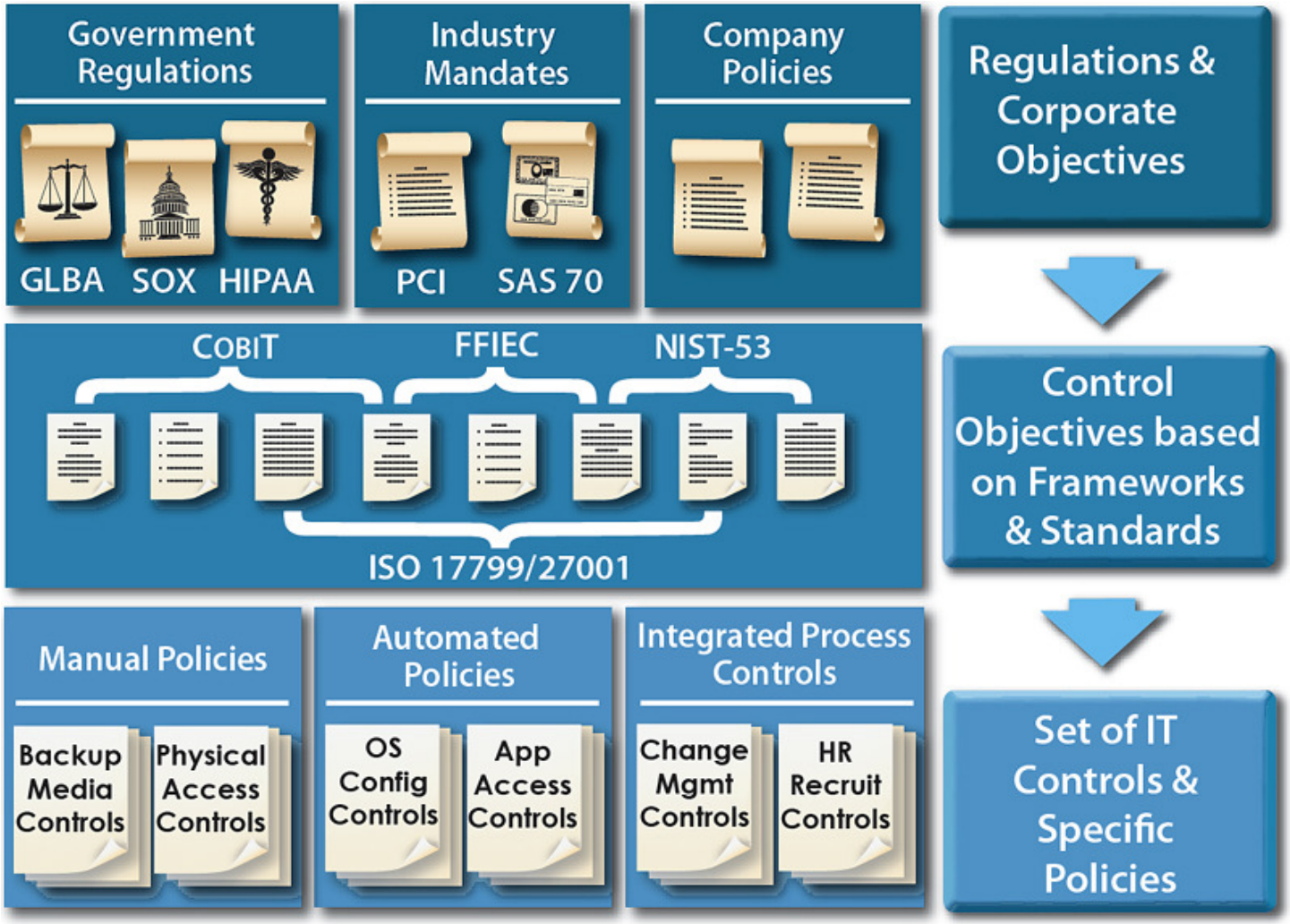
- Geschäftsführer der it.sec GmbH & Co. KG
- Mehr als 20 Jahre Berufserfahrung im IT-Security Umfeld
- Member of the Board OWASP Germany
- Contributions zu Tools wie nessus, nmap, nikto
- Etc.

Compliance, Risiko und Sicherheit

Compliance & Risk Management

- **Compliance** bedeutet nichts anderes als
  - Konform sein mit (irgendwelchen) Vorgaben
  - i.d.R umgesetzt über Kontrollfragen (Controls)
  - Unterstützt durch Frameworks wie ISO/IEC27001, Cobit …

Compliance & Risk Management



Compliance & Risk Management

- Zusammenhang zwischen Compliance & Risiko:
  - Erfüllte Controls können Risiken reduzieren
- Compliant = sicher?
  - Möglicherweise

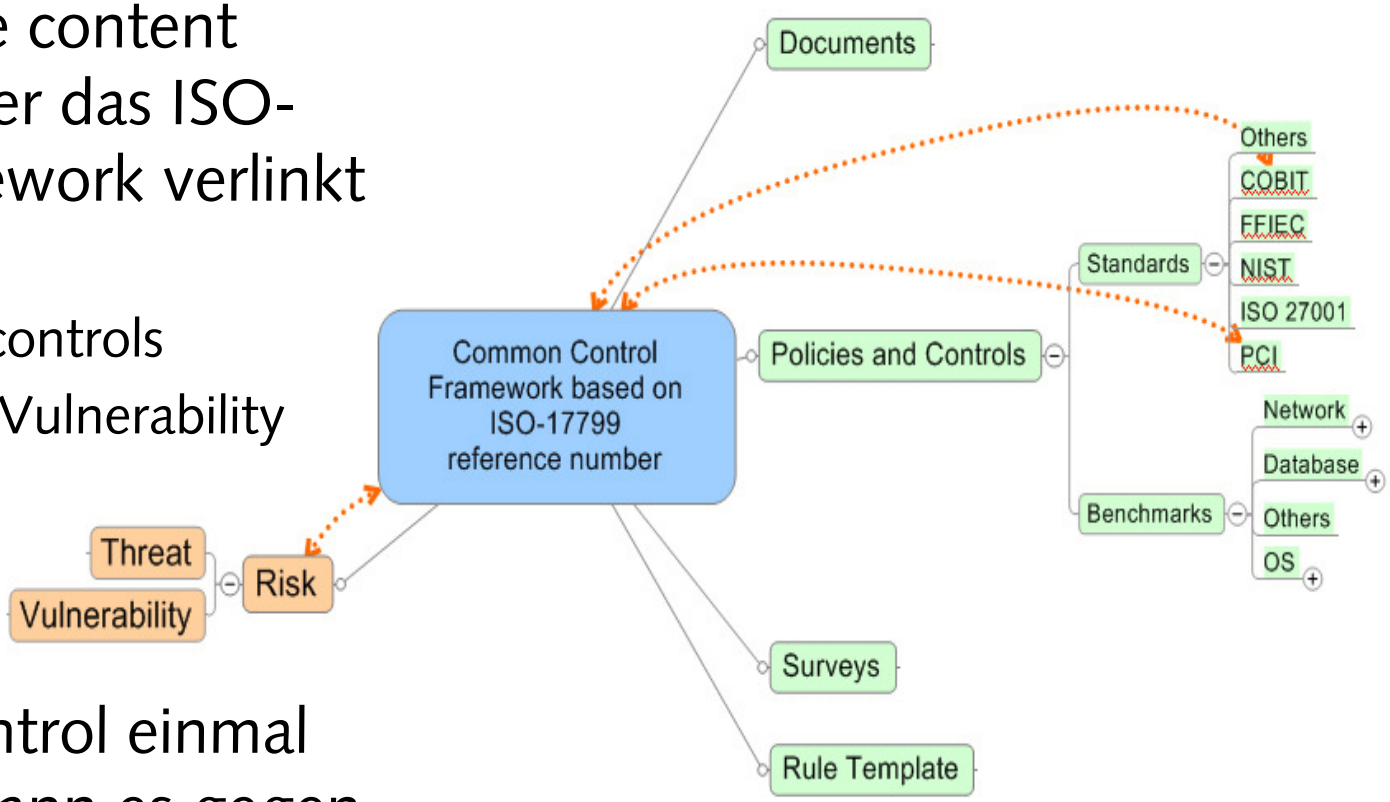
Compliance heute

- Teils immense Ressourcenanforderungen durch Audits und Compliance Management
- Immer wiederkehrende Fragen
- Kaum Automatisierung
- Verschiedene Abteilungen/Personen erarbeiten immer wiederkehrende Dinge
- Erhebung von Daten durch individuelle Befragungen
- Security und Compliance Angaben i.d.R. nur tagesgenaue Samples
- Kaum Detailgenauigkeit bei großen Umgebungen

Tools sollen helfen

Agiliance

- Die Agiliance content library ist über das ISO-17799 framework verlinkt
  - Standards
  - Automated controls
  - Risk\Threat\Vulnerability
  - andere



- Wird ein Control einmal bearbeitet, kann es gegen unterschiedliche Kataloge getestet werden

Tooleinsatz:

- Vorteile / Vision:
  - Gemeinsame Datenbasis für unterschiedliche
    - Abteilungen
    - Anforderungen
  - Konsistente(re) Datenbasis
  - Gemeinsame up-to-date Risikokataloge
  - Bessere und schellere Aussagen über Compliance & Risk
  - Aufwandsminierung

Der Kunde

Der Kunde

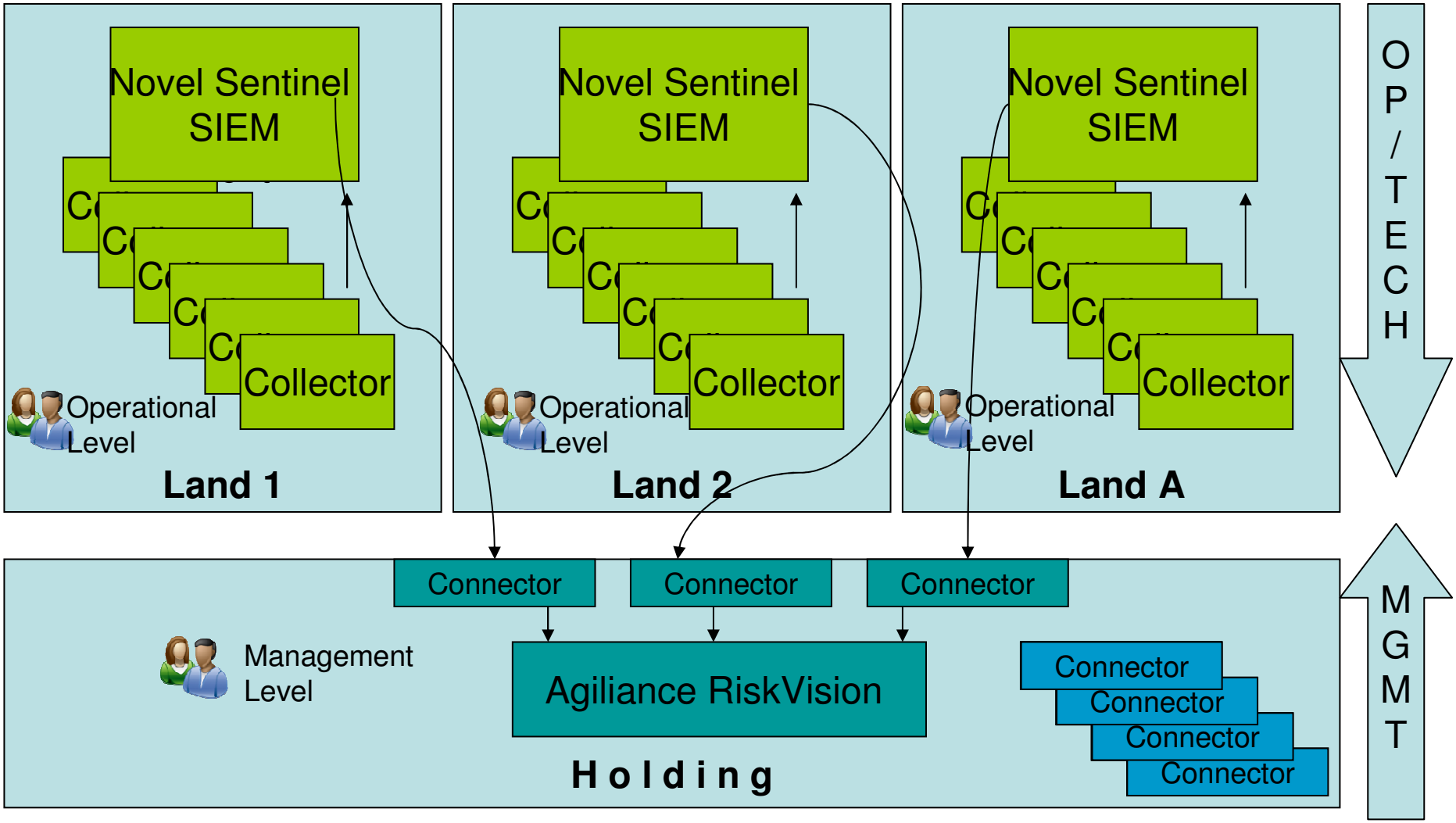
- International aufgestellter Bankenkonzern
- Töchterunternehmen (i.d.T. Banken) in *mehr als* neun Ländern
  - Töchter i.d.R. gekaufte, vormals selbstständige Banken
- Holdingstruktur
- Insgesamt einige zehntausend Mitarbeiter
- Mehr als 3000 Filialen
- Cross-Country Outsourcing
  - von den Banken in (partiell) Bankeneigene Töchter
  - für Dritte von einzelnen Banken/Töchtern

Das Projekt

Das Projekt

- entstanden aus der Anforderung nach Log-Management
- Nach drei Jahren Anforderungevolution
  - Eines gruppenweites *Security/Risk/Compliance Monitoring* Projekt
  - Getrieben durch SecMgmt der Holding
  - Operativ bei Technikern angesiedelt
  - Partner- und Produkwahl nach PoC
- Projekt gestartet (Unterschrift)
  - Pünktlich zur Bankenkrise Ende 2008
  - Geplante Laufzeit: 5 Jahre
- Umfeld
  - KEIN Gruppenprojekt
  - Budgetlage volatil
  - Unterstützung der Projektziele durch beteilige ebenfalls volatil
  - Managementsupport ebenfalls volatil
  - Dadurch: Projektschritte in abgestimmten Einzelschritten
- Projektziel
  - Nicht genau definiert
  - Muss teilweise noch nebst Teilzielen „verkauft“ werden

Vereinfachte Struktur



Die Umsetzung

Theoretischer Ablauf (vereinfacht)

- In Anlehnung an Projektziele Projekt planen, z.B:
  - Anforderungen/Requirements erheben
  - Assets erheben und definieren
    - Kritikalitäten und Loss Values definieren
  - Assets auf passende Controls Frameworks mappen, bzw. diese erstellen
  - Risikokataloge erheben und zuordnen
  - KRIs, KIPs erheben
  - Controls aus zutreffenden Frameworks/Control Lists auf Assets zuordnen
  - Hinterlegen in Agiliance (inkl. Usermanagement, Rollen etc.)
  - Alles mit Arbeitspaketen und Budgets unterlegen

Praxis

- Investitionen in das ursprüngliche Design fanden nicht statt – ursprüngliches Design nicht in-place

- „Wir brauchen Quick-Wins, ausserdem fordert PCI-DSS ein Logfile Management und da steht ein Audit an“
  - Projekt nicht auf Grüner Wiese
  - Chronologisch korrektes Vorgehen nicht unbedingt möglich

- Grundlagenprobleme
  - Verständnis für den Aufbau einer Holdingstruktur und den hieraus resultieren Anforderungen kaum vorhanden
  - Kaum Requirement-Kataloge vorhanden
  - Es gibt kein gruppenweites Verständnis (Policiy) für *Assets, Risiken, etx.*
  - Sparen, koste es was es wolle: Lizenzen

- Technische Herausforderungen
  - Single-Sign on Anforderungen in einer Non-Single-Sign-On Umgebung
  - Auswahl der funktionstragenden Komponenten (Produktfeatures überlappen)

Praxis

- Politische Probleme
  - Innenpolitisch
    - Herausarbeiten von gemeinsamen Anforderungen verschiedener Abteilungen
      - OpRisk
      - Risk
      - Legal
      - Datenschutz
      - Fraud …
    - „Aber wir haben schon ein Tool“ oder „Ihr Tool kann aber keinen Export in OpenOffice“
  - Außenpolitisch
    - Nichts menschliches ist uns Fremd (Interferenzen mit lokalen Projekten)
    - Länderzusammenarbeit schwierig
      - Z.B. Tschechien/Slowakei aus historischen Gründen
      - Geben und nehmen
    - Kein Gruppenprojekt:
      - Kein zentrales Projektmanagement
      - Kein „Häuptling“
      - Kein Fixes Budget
    - Nicht zwangsweise gemeinsames Wünsche: Transparenzfurcht

Folgen

- Homöopathisches Vorgehen
  - Lobbyarbeit
  - Verabreichung kleiner „Funktionalitäts“-Dosen
  - Schmackhaft machen und einfangen von Stakeholder durch „Köder“
- Kaum „chronologisches korrektes“ Vorgehen möglich
  - Planung folgt teils der Implementierung
  - Teils mehrere Anläuft wg. mangelnder Grundlagen vs. Quick-wins

Lessons Learned

- Die schwierigen Probleme sind in der Regel nicht die technischen
- (IT-) GRC Projekte
  - kosten Geld
  - schüren Ängste vor zu viel Transparenz
  - Kratzen oft an Bestehendem
  - Brauchen Management-Support
- Projektteile müssen „verkauft“ werden
  - Politischer Overhead ist immens
  - Stakeholder sind potentiell alle hierachischen Ebenen

Wo steht das Projekt

- Verschiedene Abteilungen der Holding suchen Anschluss
  - OpRisk und SecMgmt
  - Implementierung von Projektfreigabesurveys
  - Implementierung von KRI, KPI Erfassungen
- Holding streut „Köder“
- Länder werden auf „Anschluss“ vorbereitet
  - Requirement Assessment wurde partiell durchgeführt
  - Implementierung des Sentinel wird nun auch an Anforderungen angepasst

Fragen/Diskussion

it.sec GmbH & Co. KG
Sedanstraße 10
D-89077 Ulm

USt Id Nr.: DE 225547544
Steuernummer: 88012/53709
Amtsgericht Ulm: HRA 3129

vertreten durch den **Geschäftsführer Dipl. Ing. (FH) Holger Heimann**.

Haftender Komplementär:
it.sec Verwaltungs GmbH
Amtsgericht Ulm: HRB 4593
Sedanstr. 10
D-89077 Ulm