



Delegieren von IT- Sicherheitsaufgaben Regeln und Grenzen

Pierre Brun

Zürich

Inhalt



Relevante IT-Sicherheitsaktivitäten



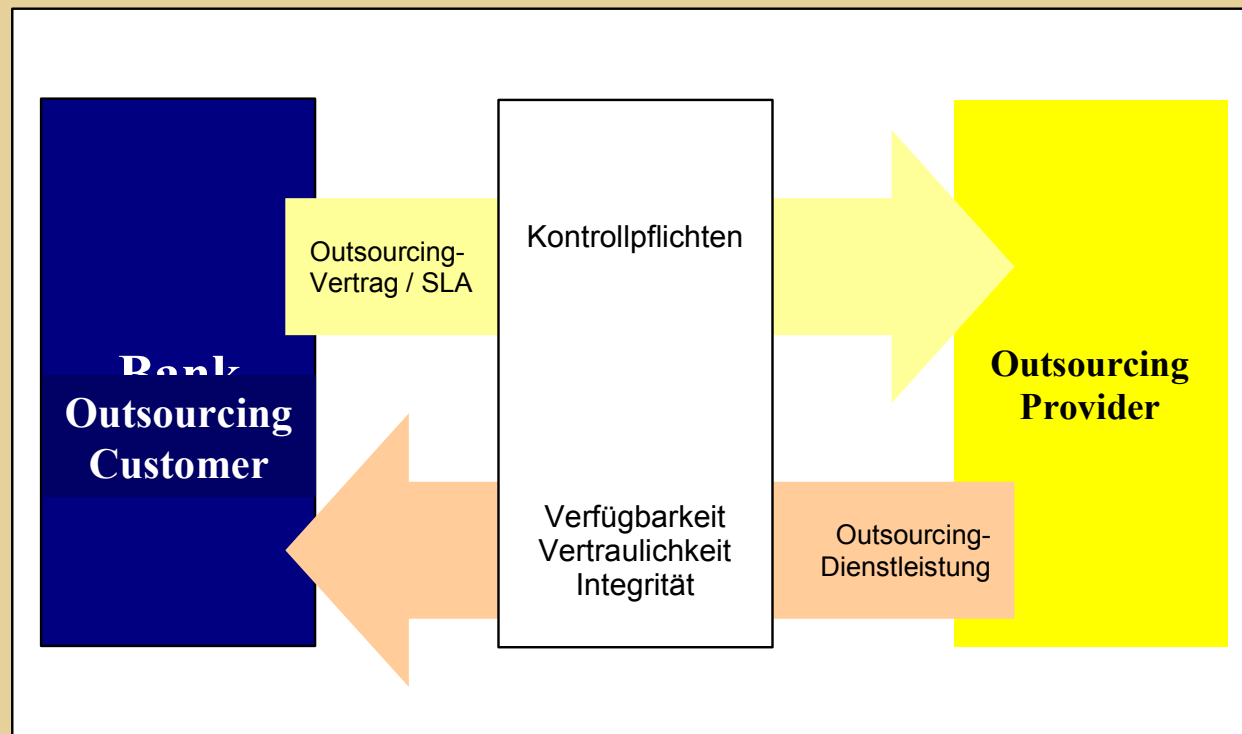
Verantwortlichkeit von IT



Regulatorisches Umfeld

Verantwortung und Outsourcing

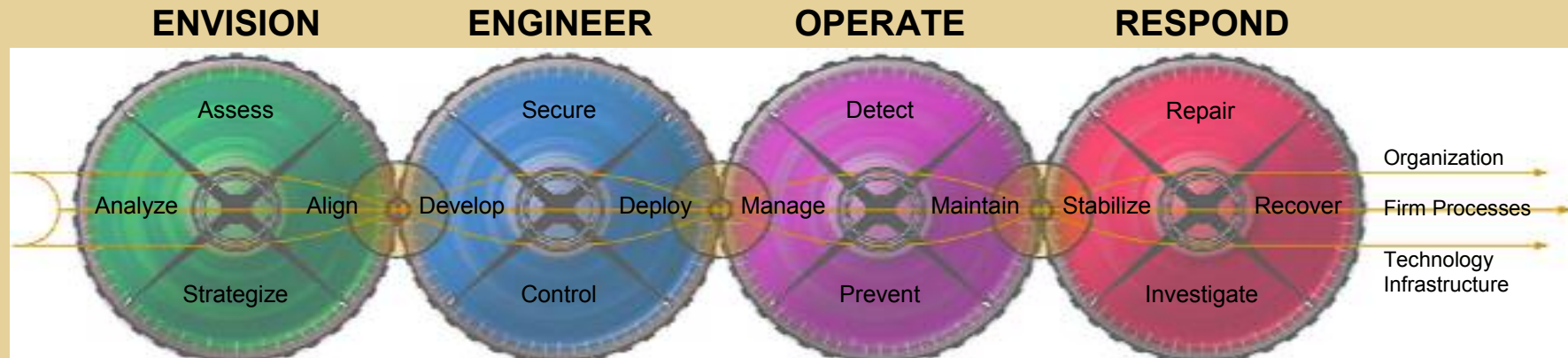
*Aufgaben und Verantwortlichkeitsbereiche der Unternehmens-IT:
Datenverarbeitung für die Geschäftseinheiten; Unterhalt der dafür
notwendigen technischen Infrastruktur und Prozesse; Einhalten von
best-practice.*



IT-Sicherheitsbegriff

- Zuverlässigkeit der technischen Infrastruktur
- Menschliche Verhaltensweisen
- Verfügbarkeit, Integrität, Vertraulichkeit von Information
- Aktualität, Zuverlässigkeit, Kohärenz, Zugreifbarkeit von Information
- Vermeidung von Schäden
- Risikominimierung

IT-Sicherheitsaktivitäten nach ESBM™



Envision	Engineer	Operate	Respond
Assess <input type="checkbox"/> Identify Business Needs <input type="checkbox"/> Appraise Information Assets <input type="checkbox"/> Valuate Risk Tolerance <input type="checkbox"/> Develop Cost Model	Secure <input type="checkbox"/> Authorize Resources <input type="checkbox"/> Establish Authentication Mechanisms <input type="checkbox"/> Grant Entitlements <input type="checkbox"/> Configure Options	Detect <input type="checkbox"/> Identify Intrusion Attempts <input type="checkbox"/> Monitor System Activity <input type="checkbox"/> Discover Unauthorized Resources <input type="checkbox"/> Detect Malicious Programs	Repair <input type="checkbox"/> Identify Root Cause <input type="checkbox"/> Eliminate Vulnerability <input type="checkbox"/> Improve Security Posture
Align <input type="checkbox"/> Monitor Strategy <input type="checkbox"/> Create Security Road Map <input type="checkbox"/> Establish Security Governance <input type="checkbox"/> Align Financial Budget <input type="checkbox"/> Assess Security Value	Deploy <input type="checkbox"/> Implement Secured Infrastructure <input type="checkbox"/> Integrate & Test Technologies <input type="checkbox"/> Deploy Security & Privacy Policies <input type="checkbox"/> Provide Training & Awareness	Maintain <input type="checkbox"/> Counteract Threats <input type="checkbox"/> Track Incidents <input type="checkbox"/> Implement Upgrades & Patches <input type="checkbox"/> Maintain Security Configurations	Recover <input type="checkbox"/> Resume Operations <input type="checkbox"/> Perform Postmortem <input type="checkbox"/> Communicate Recovery <input type="checkbox"/> Reevaluate Security Strategy
Strategize <input type="checkbox"/> Identify Security Opportunities <input type="checkbox"/> Determine Operational Impact <input type="checkbox"/> Evaluate Support Capabilities <input type="checkbox"/> Develop Strategy	Control <input type="checkbox"/> Establish Control Framework <input type="checkbox"/> Identify Roles <input type="checkbox"/> Assign User Roles	Prevent <input type="checkbox"/> Research Security Intelligence <input type="checkbox"/> Monitor Standards Compliance <input type="checkbox"/> Maintain Operational Resilience <input type="checkbox"/> Scan & Test for Vulnerabilities	Investigate <input type="checkbox"/> Preserve Evidence & Litigate <input type="checkbox"/> Determine Legal Implications <input type="checkbox"/> Appraise Impact <input type="checkbox"/> Perform Forensic Analysis
Analyze <input type="checkbox"/> Analyze Cost of Ownership <input type="checkbox"/> Define Resource Requirements <input type="checkbox"/> Prioritize Initiatives	Develop <input type="checkbox"/> Set Technical & Control Objectives <input type="checkbox"/> Classify Resources <input type="checkbox"/> Develop User Repositories <input type="checkbox"/> Define Access Control Model	Manage <input type="checkbox"/> Administer Identity Infrastructure <input type="checkbox"/> Update Standards & Policies <input type="checkbox"/> Manage Technology Infrastructure <input type="checkbox"/> Report Security Status	Stabilize <input type="checkbox"/> Assess Risk Exposure <input type="checkbox"/> Minimize Threat Impact <input type="checkbox"/> Protect Business Operations

Regulatorisches Umfeld

Die regulatorische Dichte nimmt weltweit zu. Adäquate Berücksichtigung der geltenden Vorschriften im IT Outsourcing ist ein unerlässlicher Bestandteil des unternehmensweiten Risiko-Management und trägt zur Nachhaltigkeit bei.



- Nationale Gesetze und Vorschriften
- Regionale Besonderheiten
- Kontroll-Standards
- Branchenvorschriften
- Überwachungs-Organen
- Firmen-interne Policies und Standards

Beispiel: Rundschreiben der EBK

Auslagerung von Geschäftsbereichen vom
26. August 1999, Änderungen vom 22. August 2002

Schnittstellen

Verantwortung

Zuständigkeiten

Haftungsfragen

Beispiel: Nationale Vorschriften

Schweiz: Datenschutzgesetz

EU/UK: Data Protection Acts

US: Safe Harbour

US: Corporate Information Security
Accountability Act (proposed)

California: SB1386

China: Secrecy Regulations

India: Information Technology Act 2000

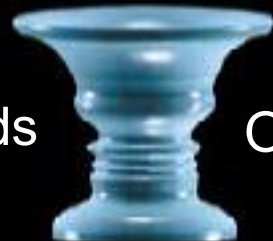
Ihre Kontaktpersonen

PricewaterhouseCoopers
Pierre Brun
Nordstrasse 15
CH-8035 Zürich
Tel. +41 1 630 2750
Fax +41 1 630 2755
pierre.brun@ch.pwc.com

PricewaterhouseCoopers
Frank Heinzmann
Nordstrasse 15
CH-8035 Zürich
Tel. +41 1 630 2766
Fax +41 1 630 2755
frank.heinzmann@ch.pwc.com

PRICEWATERHOUSECOOPERS 

Your worlds



Our people