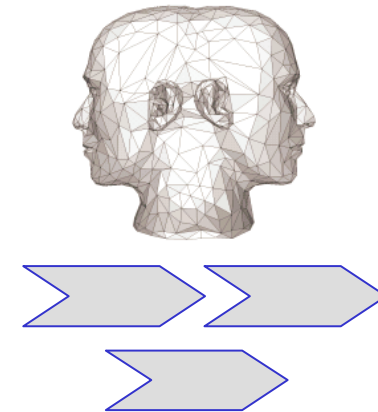




generische Prozesse für das
Identity- und Access Management



Task Force Compliance - Update

Version 1.0

- ↳ Entstanden aus Diskussion um „NIFIS-GeneriIAM-Compliance-Checkliste“ (Dez. 2006)
- ↳ Formulierte Ziele (März 2007)
 - ↳ Sammlung weiterer Informationen zum Thema Compliance
 - ↳ Zusammenfassen der gewonnenen Arbeitsergebnisse in einer Präsentation (mittelfristiges Ziel)
 - ↳ Erarbeiten einer Identity und Access Management Readyness Checkliste (langfristiges Ziel)
- ↳ Erste Präsentation auf 5. GeneriIAM Meeting in Düsseldorf
- ↳ Erstes Feedback
 - ↳ Der Aspekt wie die Compliance Anforderungen die generischen Prozesse beeinflussen muss klarer herausgearbeitet werden
 - ↳ Problem: sehr viele, sehr unterschiedliche Regelungen, die teilweise auch Branchen-/Zielgruppenspezifisch sind -> Einfluss der Compliance Anforderungen auf generische IAM-Prozesse nicht abbildbar!

Häufig sind mehrere Regelwerke zu beachten



<p>Übergreifende Regelwerke</p> <ul style="list-style-type: none"> ■ SOX ■ PIPEDA ■ Canada Multilateral Instrument 52-111 ■ CA SB-1386 ■ EU Data Protection Directive 	<p>■ HIPAA</p>  <p>Gesundheit</p>	 <p>Energie</p>	<p>■ FISMA (US)</p> <p>■ NIST 800-53</p> <p>■ Canadian and Asian Privacy Laws</p>  <p>Öffentliche Verwaltung</p>	 <p>Umwelt und Chemie</p>
<p>Finanzwesen</p> <ul style="list-style-type: none"> ■ GLBA* and USA Patriot Act ■ Basel II ■ PCI/DSS* ■ NASD 3010/3110 ■ MiFiD ■ Solvency II 		<p>Energie</p> <ul style="list-style-type: none"> ■ NERC CIP 1300 ■ Energy Bill of 2005 		<ul style="list-style-type: none"> ■ FDA 21 CFR 11

Beispiele für externe Anforderungen



Corporate Governance (einschl. Deutscher Corporate Governance Kodex)									
IT-Compliance					IT-Governance				
Gesetzliche / Behördliche Anforderungen				Selbstregulierung			Sektorspezifische Anforderungen		
Steuerrecht	Datenschutz	Anleger-schutz	Sonstige Gesetze und Verordnungen	Experten	Industrie	Finanzdienst-leister	Medizin	u.w.m.	
- UStG / SigG, SigV - AO <u>BaFin.</u> - GDPdU - GOB - GoBS	- BDSG - TMG - TKG - UrhG (GoBS/ GDPdU) - ZKDSG	- HGB - KonTröG - AktG - UMAG - IFRS	- BetrVG - BildSch - ArbVO - UWG - SGB - SRVwV - BGB - VwVIG - StGB - ElektroG	- IDW FAIT - BSI - AWW	- ITIL - HBVI - ISO - COSO - CobiT	<u>BaFin.</u> - RS 11/2001 Outsourcing - RS 18/2005 MaRisk - KWG - WpHG Umsetzung Basel-II	- MPG	- PCI DSS - AIS - CISP - SDP	
<u>EU / Intern. (USA)</u>		- Tread Act - DoD 5015.2 - NERC - Whistleblowing	- Gramm-Leach-Bliley Act (GLBA) - EU-Anti-Terror-VO - US Patriot Act - Security Breach Information Act			- Basel II - Solvency II - Banken-RiLi - Kapital-adequanz-RiLi - FISMA - GLBA	- HIPAA - FDA		

- ☾ Gibt es einen Einfluss auf die generischen IAM-Prozesse?
 - Woraus lässt sich dieser ableiten?
 - Gibt es eigenständige generische Prozesse, die sich aus Compliance Anforderungen ableiten lassen?
- ☾ Gibt es Möglichkeiten der Fokussierung?
- ☾ Wie soll weiter verfahren werden?

