



 Fachhochschule Nordwestschweiz  
 Hochschule für Wirtschaft



**Compliance – Anspruch und Wirklichkeit**

17th Symposium on Privacy and Security 2012  
 ETH Zürich, 29. August 2012

Prof. Dr. Stella Gatzu Grivas  
 Leiterin Kompetenzschwerpunkt Cloud Computing  
 Hochschule für Wirtschaft, Fachhochschule Nordwestschweiz


 Fachhochschule Nordwestschweiz  
 Hochschule für Wirtschaft

**Quellen für das Referat**

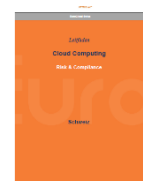

Forschungsarbeiten am Kompetenzschwerpunkt Cloud Computing im Bereich Cloud Life Cycle im Projekt CLiCK

*Unser Ziel:* Unternehmen beim Einsatz von Cloud Computing zu unterstützen

«Cloud Computing Leitfaden: Risk & Compliance», Euro Cloud Swiss ([http://www.eurocloudswiss.ch/images/stories/brochures/2012\\_EuroCloud\\_Leitfaden\\_CH\\_final\\_b.pdf](http://www.eurocloudswiss.ch/images/stories/brochures/2012_EuroCloud_Leitfaden_CH_final_b.pdf))

- Chancen und Risiken
- Compliance mit Fokus auf Personendaten
- Auslagerung von Daten an Dritten und ins Ausland
- Beispiele (Banken, Industrieunternehmen, Telekommunikationsprovider)
- Vertragsgestaltung
- IT Sicherheit

Studie von Ponemon Institute durchgeführt in Juli 2012 in Deutschland bei kleinen und mittleren Organisationen gesponsert von Microsoft (<http://www.microsoft.com/germany/newsroom/pressemitteilung.msp?id=533599>)

---

Kompetenzschwerpunkt Cloud Computing FHNW
2

**n w** Fachhochschule Nordwestschweiz  
Hochschule für Wirtschaft

### Cloud Computing überall und in jeder Form

- gute Definitionen auch auf youtube:  
[http://www.youtube.com/watch?feature=player\\_embedded&hl=de&v=ae\\_DKNwK\\_ms](http://www.youtube.com/watch?feature=player_embedded&hl=de&v=ae_DKNwK_ms) oder <http://www.youtube.com/watch?v=mefUnG4BNPs>
- Cloud Computing ist mehr als Outsourcing, Virtualisierung oder Application Service Provider
- kann für eine Firma aber auch für eine Privatperson ein Thema sein
- ist in beliebigen Domänen einsetzbar (<http://www.youtube.com/watch?v=8PkbbCf07Co>)
- kann in Form eines beliebigen Service angeboten werden (Music as a Service)
- ist da und ist in aller Munde (Konferenzen, Veranstaltungen, im Internet, in der CIO Agenda – auch bei Gartner's CIO Agenda  
<http://www.cioinsight.com/c/a/IT-Management/Gartner-2012-CIO-Agenda-Survey-882188/>, Teil von vielen Umfragen, Artikeln, Paneldiskussionen)
- **ist aber kein Heilmittel für alles und kann je nach Einsatz auch Nachteile mit sich bringen (wie Kostensteigerung, Herausforderung bei der Migration und Integration oder bei der Compliance)**

---

Kompetenzschwerpunkt Cloud Computing FHNW 3

**n w** Fachhochschule Nordwestschweiz  
Hochschule für Wirtschaft

### Der Weg in die Cloud – Grundlegende Fragen für Unternehmen als Cloud-Anwender

- Welche Einflüsse hat Cloud Computing auf meinem Unternehmen?
  - IT Organisation, Governance, Risiko Management, Compliance
  - IT Landschaft
  - Partnerschaften
  - IT Kosten
  - Geschäftsentwicklung
- Welche Chancen und Risiken gehe ich ein?
- Welche sind für mich die «richtigen» Anbieter?
  - Welche Angebote gibt es am Markt?
  - Welche Angebote machen für mich Sinn aus strategischer, politischer und wirtschaftlicher Sicht?
- Wie können solche Angebote in meine heutige IT Umgebung integriert werden?
  - Brauche ich eine Migrationsstrategie?
  - Wie soll eine solche Migration durchgeführt werden?

---

Kompetenzschwerpunkt Cloud Computing FHNW 4

**n w** Fachhochschule Nordwestschweiz  
Hochschule für Wirtschaft

### IT Compliance

**IT Compliance**  
Einhaltung der gesetzlichen, unternehmensinternen und vertraglichen Regelungen im Bereich der IT-Landschaft rund um die IT-Sicherheit, Verfügbarkeit, Datenaufbewahrung und Datenschutz

Kompetenzschwerpunkt Cloud Computing, FHNW 5

**n w** Fachhochschule Nordwestschweiz  
Hochschule für Wirtschaft

### IT Compliance in Abhängigkeit mit IT Governance und IT Risiko Analyse

```
graph TD; IG[IT Governance] <--> ITA[IT Risiko Analyse]; IG <--> IC[IT Compliance]; ITA <--> IC;
```

**IT Governance**  
Führung, Organisation, Verantwortlichkeiten und Prozesse

**IT Risiko Analyse**  
Analyse und Bewertung der strategischen Problemen

**IT Compliance**  
Einhaltung der gesetzlichen, unternehmensinternen und vertraglichen Regelungen im Bereich der IT-Landschaft rund um die IT-Sicherheit, Verfügbarkeit, Datenaufbewahrung und Datenschutz

Kompetenzschwerpunkt Cloud Computing, FHNW 6

**n w** Fachhochschule Nordwestschweiz  
Hochschule für Wirtschaft

## Cloud Computing und Datenschutz

- **«Datenschutz bezeichnet den Schutz des Einzelnen vor dem Missbrauch personenbezogener Daten»**
  - Der Begriff wurde auch verwendet für den Schutz wissenschaftlicher und technischer Daten gegen Verlust oder Veränderung – und Schutz gegen Diebstahl dieser Daten
- **Das Bundesgesetz über den Datenschutz (DSG) ist das Datenschutzgesetz der Schweiz. Es bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen und juristischen Personen, über die Daten bearbeitet werden ( SR 235.1 Bundesgesetz über den Datenschutz) ( [http://www.admin.ch/ch/d/sr/235\\_1/index.html](http://www.admin.ch/ch/d/sr/235_1/index.html))**
- **Cloud Computing» ist auch «Datenverarbeitung in der Wolke»**
  - über Netze angeschlossene Rechnerlandschaft, in welche die eigene Datenverarbeitung ausgelagert wird

---

Kompetenzschwerpunkt Cloud Computing FHNW 7


**n w** Fachhochschule Nordwestschweiz  
Hochschule für Wirtschaft

## Cloud Computing und IT Compliance – Drei typische Fragen

- **Stellt der Einsatz von Cloud Computing zusätzliche Compliance-Aufgaben an einem Unternehmen?**
  - Unterschiede zu Outsourcing?
- **Wer hat für IT Compliance zu sorgen? Wer trägt die Verantwortung?**
  - Gemäss Eidgenössischem Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB):  
«Unternehmen und Behörden, die solche Dienste in Anspruch nehmen, sind sich oft zu wenig bewusst, dass die primäre Pflicht zur Einhaltung der Datenschutzregeln zunächst einmal bei ihnen selbst liegt und nicht beim Anbieter, der die Daten auf einem Cloud-Server speichert oder in der Cloud bearbeitet»
- **Welche ist die Rolle des Cloud-Providers?**
  - TRUST schaffen, indem der Cloud-Provider für die Sicherheit der Daten sorgt
  - Einhaltung vertraglicher Zustimmungen

---

Kompetenzschwerpunkt Cloud Computing, FHNW 8


 Fachhochschule Nordwestschweiz  
 Hochschule für Wirtschaft

---

**Cloud Computing und Outsourcing: Grundlegende Unterschiede**


---

Veränderungen im Serviceeinkauf		
Kriterium	Klassisches Outsourcing	Cloud Computing
Services	Services sind auf Kunden abgestimmt	Services sind vom Provider standardisiert, industrialisiert, automatisiert und skalierbar
Service Level	Individuell	Provider bestimmt Standard
Technologie	Mitbestimmung durch Kunde	Provider bestimmt Standard
Releasemanagement	Mitbestimmung durch Kunde	Provider bestimmt Standard
Vertrag	Kunde gibt vor	Provider bestimmt Standard
Preismodelle	Kunde gibt vor	Provider bestimmt Standard
Standort der Daten	Mitbestimmung durch Kunde	Provider bestimmt Standard
Betreuung	Ansprechpartner	Selbstbedienung durch den Kunden über Web Portale

**Soberano Sourcing Workbook / © Soberano**

---

Kompetenzschwerpunkt Cloud Computing FHNW 9


 Fachhochschule Nordwestschweiz  
 Hochschule für Wirtschaft

---

**Unterschiede zu Outsourcing – Rechl. Rahmenbedingungen in Bezug auf die Daten**

---

- Auslagerung der Daten im Ausland:
  - Kontrollverlust grösser als im Inland
  - Gemäss schweizerischem Recht müssen Länder, in welche Personendaten ausgelagert werden, das gleiche datenschutzrechtliche Niveau bieten wie die Schweiz (in EU-Ländern wie Deutschland gewährleistet).
  - USA erreicht das datenschutzrechtliche Niveau der Schweiz nicht
  
- Datenbearbeitung durch Dritte:
  - Das schweizerische Recht ermöglicht natürlichen sowie juristischen Personen zu bestimmen, von wem, ob und wie ihre Daten verarbeitet werden.
  - Handelt es sich bei den zu migrierenden Daten um Personendaten, können besondere Geheimnispflichten bestehen (z.B. Bankgeheimnis).
  
- Besondere Regulierung:
  - Regulierungen verlangen unter Umständen besondere Massnahmen (z.B. bei Finanzdienstleistern, Dienstleistern des Gesundheitswesens, Versicherungsdienstleistern etc.).

---

Kompetenzschwerpunkt Cloud Computing, FHNW 10

**n w** Fachhochschule Nordwestschweiz  
Hochschule für Wirtschaft

### Rolle vom Cloud Provider – TRUST schaffen aber wie?

Cloud Anwender ← **Anwender vertraut Anbieter blind** → Cloud Provider

Cloud Anwender ← **Anwender macht es allen recht** → Cloud Provider

Cloud Anwender ← **Individuelle Abstimmung – Der Vertrag** → Cloud Provider

Cloud Anwender ← **Standards, Richtlinien und Zertifizierungen** → Cloud Provider

Cloud Anwender ← **zusammen auftreten in einer Community** → Cloud Provider

Cloud Anwender ← **«intelligente Systeme» als Intermediators** → Cloud Provider

---

Kompetenzschwerpunkt Cloud Computing FHNW 11

**n w** Fachhochschule Nordwestschweiz  
Hochschule für Wirtschaft

### Kein «blindes Vertrauen»: Cloud Anwender trägt die Verantwortung

**Der Cloud Anwender ist die verantwortliche Stelle und bleibt für die Einhaltung sämtlicher datenschutzrechtlicher Bestimmungen verantwortlich**

**Der Cloud Anwender muss einen schriftlichen Auftrag an den Cloud Anbieter erteilen, damit er die inhaltlichen Anforderungen erfüllen kann**

- Eine Verletzung seitens Cloud Anbieters muss strafrechtliche Folgen haben
- Die Einbeziehung von Unter-Anbietern kann für den Cloud Anwender intransparent sein

**Der Cloud Anwender hat sich regelmässig von der Einhaltung der beim Cloud Anbieter als Auftragnehmer getroffenen technischen und organisatorischen Massnahmen zu überzeugen.**

- Dem Cloud Anwender wird es dabei nicht immer möglich sein, eine Vor-Ort-Prüfung durchzuführen
- Eine blosse Zusicherungen des Cloud Anbieters ist nicht ausreichend
- Eine Zertifizierung bei einer unabhängigen und kompetenten Prüfstelle von Cloud Anbietern könnte eine Lösung sein ([Aktivitäten von EuroCloud Swiss](#), [Zertifikat für SaaS](#))
- Das Vorliegen von Zertifikaten entbindet den Cloud Anwender jedoch nicht von seinen Kontrollpflichten

- UND der Cloud Anwender braucht eine EXIT-Strategie!!

---

Kompetenzschwerpunkt Cloud Computing FHNW 12

Die Wahl des Cloud Providers hängt mit der Einhaltung der Sicherheitsrichtlinien

Studie von Ponemon Institute durchgeführt in Juni 2012 in Deutschland bei kleinen und mittleren Organisationen, gesponsert von Microsoft

Interviews von 668 IT-Verantwortlichen:  
 •52% direkt unter dem CIO  
 •17% direkt unter dem Compliance Officer  
 •16% direkt unter dem Chief Information Security Officer)

FIGURE 2  
IMPACT OF CLOUD PROVIDER'S PRIVACY POLICIES AND PRACTICES ON SELECTION OF CLOUD PROVIDERS

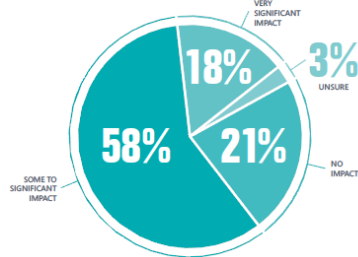
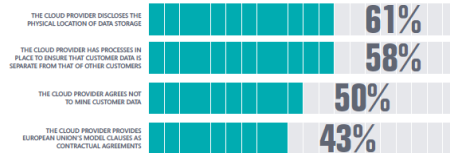


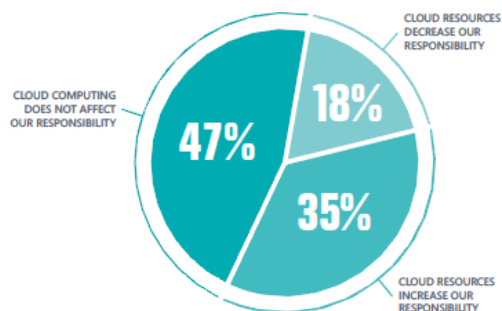
FIGURE 3  
IMPORTANT ISSUES THAT DETERMINE THE CLOUD PROVIDERS' COMMITMENT TO PRIVACY  
"VERY IMPORTANT" AND "IMPORTANT" RESPONSES COMBINED



Ponemon Studie

Aber Vorsicht:  
Haben die Unternehmen die Verantwortung an die Cloud-Provider ausgelagert?

FIGURE 7  
IMPACT OF CLOUD COMPUTING ON ORGANIZATIONAL RESPONSIBILITY TO SAFEGUARD INFORMATION



Ponemon Studie

**n w** Fachhochschule Nordwestschweiz  
Hochschule für Wirtschaft

## Der Vertrag ein MUSS – Das Kontrollinstrument des Cloud Anwenders

### 1. Ziel Nutzungsbedingungen lesen

**Nutzungsbedingungen akzeptiert**

**Nutzungsbedingungen gelesen**

### 2. Ziel: Sich Informieren

- Vor-Ort-Kontrolle meistens nicht möglich
- Anerkannte **Gütesiegel** können die Kontrolle des Anbieters erleichtern, entbinden aber nicht von der Kontrollpflicht des Cloud-Anwenders
- Bei Unter-Anbietern muss der Cloud-Anbieter vor Unterbeauftragung eine Kontrolle durchführen

Kompetenzschwerpunkt Cloud Computing FHNW 15

**n w** Fachhochschule Nordwestschweiz  
Hochschule für Wirtschaft

## Der Vertrag – Empfehlungen gemäss EuroCloud Swiss Leitfaden

Vertragsabschluss und -gestaltung	Vertragliche Massnahmen	Abbildung der Compliance Massnahmen	Abbildung der Security Massnahmen
<ul style="list-style-type: none"> <li>• online oder schriftlich</li> <li>• face-to-face Meeting</li> </ul>	<ul style="list-style-type: none"> <li>• Vergütungsregelung</li> <li>• Leistungsstörung</li> <li>• Vertragskündigung</li> <li>• Datenlöschung bei Vertragsende</li> <li>• Insolvenz des Anbieters</li> </ul>	<ul style="list-style-type: none"> <li>• Datenschutz</li> <li>• Datenarchivierung</li> <li>• Beauftragung und Weisungsrecht</li> <li>• Kommunikation und Dokumentation</li> <li>• Kontrollmöglichkeiten des Nutzers</li> <li>• Überbindung auf Subunternehmer</li> </ul>	<ul style="list-style-type: none"> <li>• Massnahmen im Rechenzentrum</li> <li>• Massnahmen betreffend Netz- und Serversicherheit</li> <li>• Massnahmen betreffend Datensicherheit</li> </ul>

Kompetenzschwerpunkt Cloud Computing FHNW 16

**n w** Fachhochschule Nordwestschweiz  
Hochschule für Wirtschaft

## Standards und Richtlinien als Lösung?

- **Standards und Richtlinien**
  - NIST (National Institute of Standards and Technology)  
<http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf>, <http://www.nist.gov/itl/cloud/index.cfm>
  - ENISA (European Network and Information Security Agency)  
<http://www.enisa.europa.eu/act/application-security/test>  
<http://www.enisa.europa.eu/activities/identity-and-trust/past-work-areas/cloud-computing/enisa-cloud-computing-risk-assessment/>
  - CSA (Cloud Security Alliance)  
<https://cloudsecurityalliance.org/>  
<https://cloudsecurityalliance.org/wp-content/themes/csa/guidance-download-box.php>  
<https://cloudsecurityalliance.org/education/certificate-of-cloud-security-knowledge/>  
<https://cloudsecurityalliance.org/star/>
  - BSI (in Deutschland: Bundesamt für Sicherheit in der Informationstechnik)  
[https://www.bsi.bund.de/DE/Themen/CloudComputing/CloudComputing\\_node.html](https://www.bsi.bund.de/DE/Themen/CloudComputing/CloudComputing_node.html)

---

Kompetenzschwerpunkt Cloud Computing FHNW 17

**n w** Fachhochschule Nordwestschweiz  
Hochschule für Wirtschaft

## Zertifizierung als Lösung?

- EuroCloud Deutschland (EuroCloud Star Audit)  
<http://www.saas-audit.de/>

**Zertifikat für Providers tätig im Schweizer Markt ist unterwegs**

- TÜV (Geprüfter Datenschutz – Cloud Computing V1.0)  
[http://www.tuv.com/de/deutschland/gk/consulting\\_informationssicherheit/strategische\\_informationssicherheit/datenschutz\\_zertifizierung\\_unternehmen/datenschutz\\_zertifizierung\\_unternehmen.jsp](http://www.tuv.com/de/deutschland/gk/consulting_informationssicherheit/strategische_informationssicherheit/datenschutz_zertifizierung_unternehmen/datenschutz_zertifizierung_unternehmen.jsp)

Mehr Informationen unter [www.trusted-cloud.de](http://www.trusted-cloud.de)

---

Kompetenzschwerpunkt Cloud Computing FHNW 18

**n w** Fachhochschule Nordwestschweiz  
Hochschule für Wirtschaft

### Community Clouds als Lösung?

- Unternehmen oder Organisationen der gleichen Branche kommen zusammen und bilden einen Community Cloud, die dann nur den Mitgliedern der Community zugänglich sind.
  - gleiche Anforderungen an Funktionalität und Anwendungen
  - gleiche Anforderungen an Security und Compliance
- Community Clouds bieten
  - Application Store (SaaS Angebote), IaaS und PaaS Angebote
  - Austausch in der Community
- Einige Beispiele aus der Verwaltung:
  - GovCloud Projekt von Informatikstrategie von Bund
  - G-Cloud Projekt von England (<http://www.cabinetoffice.gov.uk/sites/default/files/resources/08-G-CLOUD-TechnicalArchitectureWorkstrand-Report.pdf>)
- Auch in anderen Domänen sichtbar
  - Community Cloud für die Finanzindustrie, Education Cloud

---

Kompetenzschwerpunkt Cloud Computing FHNW 19

**n w** Fachhochschule Nordwestschweiz  
Hochschule für Wirtschaft

### Eine webbasierte Infoplace als Lösung?

#### CLiCK Projekt (Cloud Life Cycle) Ein «intelligentes» System als Experte

**Business Case Framework**

Area	Value	Impact	Priority	Score	Weight	Final
Business Case	High	High	High	10	10	100
Cloud Readiness	Medium	Medium	Medium	5	5	25
Use Case	Low	Low	Low	2	2	4
Provider Landscape	High	High	High	10	10	100
Cloud Readiness Assessment	Medium	Medium	Medium	5	5	25
Use Case Repository	Low	Low	Low	2	2	4
Provider Landscape	High	High	High	10	10	100
Cloud Readiness Assessment	Medium	Medium	Medium	5	5	25
Use Case Repository	Low	Low	Low	2	2	4

**Provider Landscape**  
Sign in preference across all RPX customer websites

Google: 30%, Facebook: 20%, Microsoft: 10%, Yahoo: 10%, Other: 30%

---

Kompetenzschwerpunkt Cloud Computing FHNW 20

**n w** Fachhochschule Nordwestschweiz  
Hochschule für Wirtschaft

### Wo sind wir heute? Wie wird der Cloud Provider ausgewählt?

**FIGURE 8**  
METHODS FOR VETTING OR EVALUATING CLOUD PROVIDERS  
MORE THAN ONE CHOICE PERMITTED

64% CONTRACTUAL NEGOTIATION AND LEGAL REVIEW  
52% PROOF OF COMPLIANCE  
39% SELF-ASSESSMENT CHECKLIST COMPLETED BY PROVIDER

**FIGURE 10**  
METHODS FOR SECURING CONFIDENTIAL OR SENSITIVE PERSONAL INFORMATION IN THE CLOUD  
MORE THAN ONE CHOICE PERMITTED

70% WE RELY ON ASSURANCES FROM THE CLOUD PROVIDER  
59% WE RELY ON CONTRACTUAL AGREEMENTS WITH THE CLOUD PROVIDER  
40% WE USE CONVENTIONAL DATA SECURITY TOOLS TO PROTECT INFORMATION  
10% WE BUY ADDITIONAL SECURITY SERVICES PROVIDED BY THE CLOUD PROVIDER  
9% DON'T KNOW  
2% OTHER

**FIGURE 12**  
CONDITIONS THAT AFFECT THE DECISION TO USE A CLOUD PROVIDER

43% THIRD PARTY PROVIDES ASSURANCE THAT THE CLOUD PROVIDER MEETS PRIVACY AND PROTECTION REQUIREMENTS  
55% THE CLOUD PROVIDER AGREES TO MEET ALL PRIVACY AND DATA PROTECTION REQUIREMENTS

MUCH MORE LIKELY TO BUY CLOUD SERVICES  
MORE LIKELY TO BUY CLOUD SERVICES  
NO EFFECT ON THE DECISION TO BUY CLOUD SERVICES  
UNSURE

und 38% gehen auf zertifizierte Providers

**FIGURE 9**  
MOST IMPORTANT CERTIFICATIONS USED WHEN EVALUATING CLOUD PROVIDERS  
TWO CHOICES PERMITTED

51% SAS-70  
48% PCI DSS  
43% ISO 27001  
2% OTHER

**Ponemon Studie**

Kompetenzschwerpunkt Cloud Computing FHNW 21

**n w** Fachhochschule Nordwestschweiz  
Hochschule für Wirtschaft

### Zusammenfassung

- Awareness über IT-Compliance Herausforderungen mit dem Einsatz von Cloud Services ist da!!
- Wir brauchen jedoch
  - Expertise in der Vertragsschliessung und SLAs
  - Zertifizierungen und Gütesiegel
  - Community Clouds
  - Expertenwissen allen zugänglich

Kompetenzschwerpunkt Cloud Computing FHNW 22

**n w** Fachhochschule Nordwestschweiz  
Hochschule für Wirtschaft

**VIELEN DANK FÜR IHRE  
AUFMERKSAMKEIT!**



University of Applied Sciences  
Northwestern Switzerland FHNW  
School of Business  
Institute of Information Systems

Prof. Dr. Stella Gatzu Grivas  
Head Competence Center Cloud Computing

T +41 62 286 00 58  
[stella.gatziugrivas@fhnw.ch](mailto:stella.gatziugrivas@fhnw.ch)  
<http://www.fhnw.ch/wirtschaft/iwi/kompetenzschwerpunkte/>

---

Kompetenzschwerpunkt Cloud Computing, FHNW 23