



Compliance in the Cloud

Enno Rey, Roger Klose,
Matthias Luft
{erey, rklose, mluft}@ernw.de



- **Heidelberg based security consulting and assessment company with currently 18 employees (as of Sep 2010).**

- Independent
- Deep technical knowledge
- Structured (assessment) approach
- Business reasonable recommendations
- We understand corporate



- **Blog: www.insinuator.net**

- **Conference: www.troopers.de**





Agenda

- **Trust & Control**
- **Trust – Contributing Factors**

- **Compliance**
 - Personal Data
 - SOX
 - PCI



Trust & Control

- In the end of the day what everybody involved in infosec (and, for that matter, everybody else as well) looks for is ... confidence.
- Confidence means “feeling comfortable/secure/safe”.
- This confidence can be based on two major ingredients
 - Trust 
 - Control 
- **Both are valid sources for confidence.**
 - Infosec people usually give preference for the control approach though.



Sometimes you can trust...

Home



Datacenter



...and sometimes you better control

Home



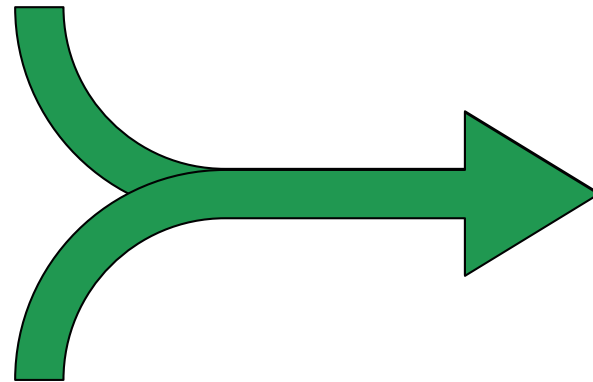
Datacenter



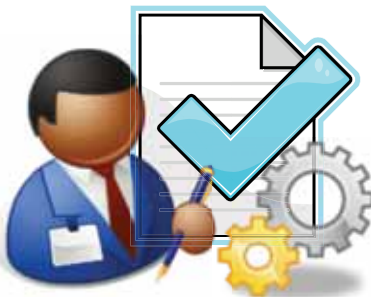
Trust, Control & Confidence



TRUST



CONFIDENCE



CONTROL



The problem of *trust*

- **Diego Gambetta:**

"trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action".

- **Something non-*subjective* might be helpful.**
- **This could be some way of documenting *reasons for trust*.**



Problems of “the control approach”

- **Costs!**



- **Operational impact**

- Business might feel obstructed.



- **Usually controls increase overall complexity**

- → might be bad for overall security.





Trust
—
Contributing Factors





Size (of entity to trust)
→ *Risk/impact factor*





Transparency
How much do we know?



Symmetry



Do they trust us?





Consistency

What happened in the past?



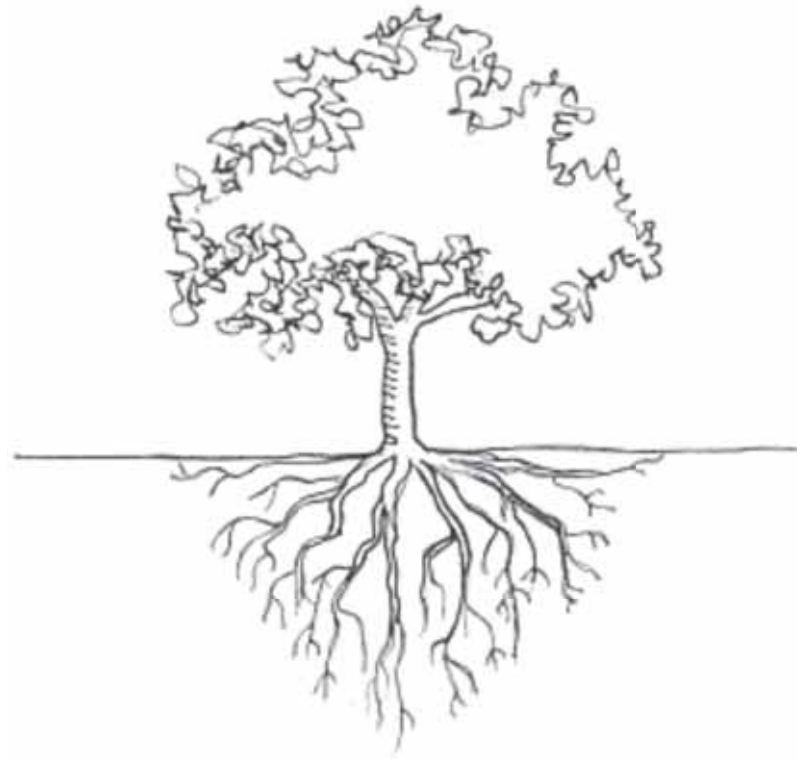
Trust, Contributing Factors



Offset: How much do they pay when they break the trust.

→ Instrument of control





Integrity

Amount and timely notice of change within target





Components

Number of elements which currently provide resources which the subject relies on

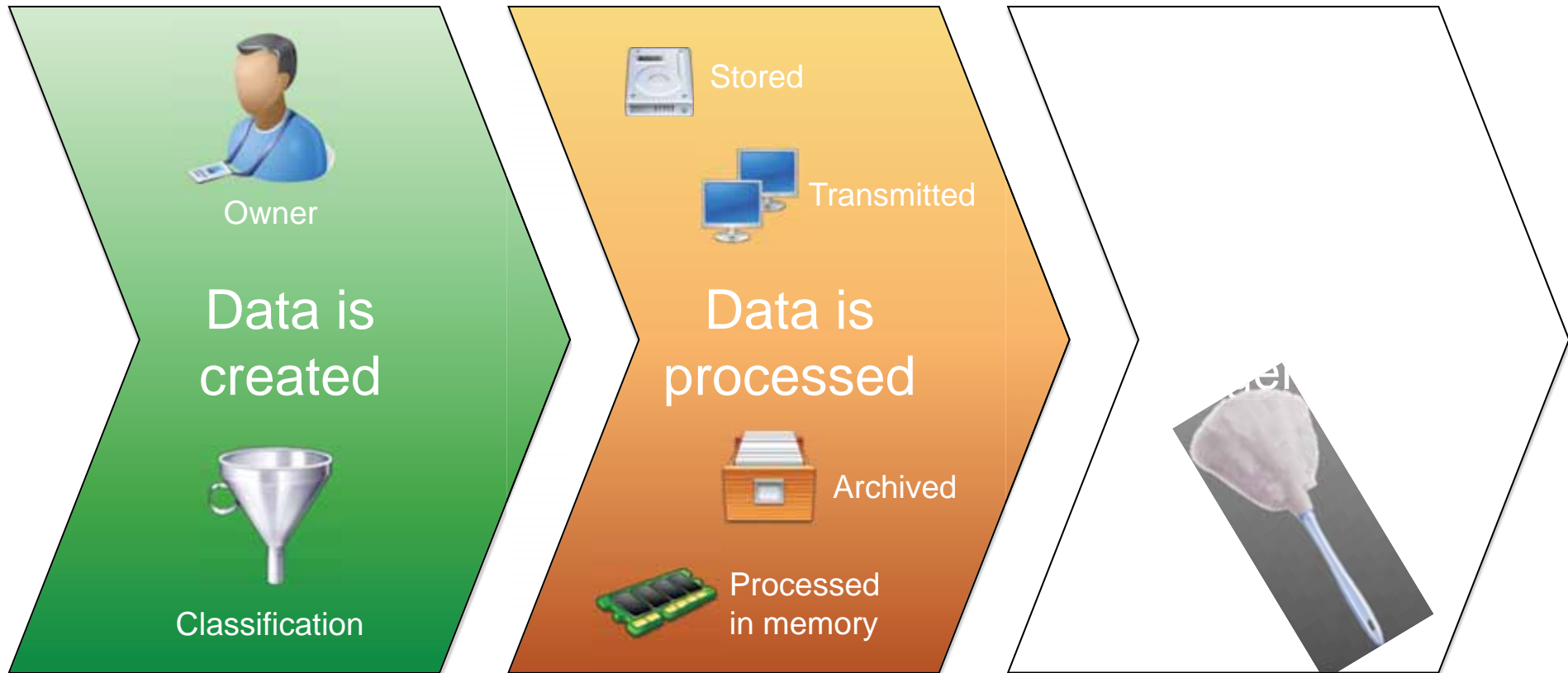




Data Lifecycle



Data Lifecycle



Compliance

Data Protection / Personal Data



Data Protection

- Not just means “protection of [some] data”, but is an idea prevalent in the Western societies.
- In the stricter, conceptual sense of the word, “data protection” means the approach of protecting certain kinds of data denoted
 - *Personal Data* [EU_DIR]
 - *Personenbezogene Daten* [BDSG]
 - *Personally identifiable information / PII* [OMB → US]
- **This data has to be protected in some way**
 - Legislation / Regulations
 - Derived common best practices in handling



Personal Data

- **[EU_DIR]: any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”.**



- **[BDSG]: “Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“.**

→ Essentially, this means: all data related to a *person*.



- **[EU_DIR]: any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination or blocking, erasure or destruction”.**
 - **[BDSG]: “Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. [...] Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten”.**
- **Essentially, this means: all operations that can be performed on this data.**



Relevant Regulations

- **Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. → [EU_DIR]**
 - Implemented in 1995 by the European Commission.
 - As EU directives are addressed to member states, no direct legal impact on citizens. The member states had to transpose the directive into internal law.
- **Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814) geändert worden ist.**



Basic Elements as of [BDSG]

- Lawful processing / *Zulässigkeit*
- Consent / *Einwilligung*
- Processing for specified, explicit and legitimate purposes / *Zweckbindung*
- Avoidance & economic handling of data / *Datenvermeidung & Datensparsamkeit*
- Right of information, correction, erasure / *Recht des Betroffenen auf Auskunft, Berichtigung, Löschung*
 - Transparency / *Transparenz*
- Security of processing (Implementation of – appropriate – measures) / *Pflicht zur Datensicherung (Durchführung von – angemessenen – Maßnahmen)*
- Control of processing in foreign countries and/or by 3rd parties / *Regelung der Verarbeitung im Ausland und/oder im Auftrag (durch Dritte)*



Right of information, correction, erasure

- **[BDSG, §34]: “Auskunft an den Betroffenen”**
- **[BDSG, §35]: “Berichtigung, Löschung und Sperrung von Daten”**
- **[BDSG, §6]: “Die Rechte des Betroffenen auf Auskunft (§§ 19, 34) und auf Berichtigung, Löschung oder Sperrung (§§ 20, 35) können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.”**
- **How to ensure this “in the cloud”?**



[BDSG, §9]: “Öffentliche und nicht-öffentliche Stellen, die [...] personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes [...] zu gewährleisten.”

The associated appendix [“Anlage (zu § 9 Satz 1)“] specifies the following:

- **Physical access control / *Zutrittskontrolle***
- **Admission control / *Zugangskontrolle***
- **Logical access control / *Zugriffskontrolle***
- **Control over dissemination / *Weitergabekontrolle***
- **Entry control / *Eingabekontrolle***
- **Order control / *Auftragskontrolle***
- **Availability control / *Verfügbarkeitskontrolle***
- **Separate processing / *Gewährleistung getrennter Verarbeitung***



Explicit mention of encryption technologies (*Verschlüsselungsverfahren*).



Control of processing in foreign countries

- **[BDSG, § 4b]: “Übermittlung personenbezogener Daten ins Ausland”**
- **Transfer to member states of EU or EEA permissible without any additional requirements.**
- **Otherwise an “appropriate level of protection” has to be ensured**
 - Covered by US-EU *Safe Harbor* framework
 - Use of *European Commission* standard contract clauses
 - Use of (company internal) *binding corporate rules* (BCRs)
- **In cloud context (EC2), use of “regions” recommended.**



Control of processing by 3rd parties

- **[BGG, §11]: “Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag”**

“Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich.“

→ You can't transfer (your) responsibility.

**“Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen.
Der Auftrag ist schriftlich zu erteilen“.**

→ The contract is important! See [BDSG, § 11] for details.



Conclusions

- **Prerequisites for processing personal data in the cloud:**
 - Contracts
 - Restrict processing to certain regions/countries (EU, US)
 - Encrypt where operationally feasible

- **Explicitly ask for CP's data protection handling.**



SOX



SOX & The cloud

- **The jury is still out on that.**
- **The prevailing opinion is that handling SOX relevant data in a (public) cloud should be avoided or at least handled *very carefully*.**
- **We are not aware of any environments which do this currently.**



- **Strictly speaking handling SOX relevant data in a (public) cloud shouldn't be a problem as long as**
 - the outsourcing organization (*_not_* the CP) can prove that *internal controls* (still) are in place.
 - Encrypt wherever possible.
 - The more logs the better.
 - CP certifications (ISO 27001, SAS 70 Type II) will certainly help.
 - Security monitoring might be helpful.



PCI

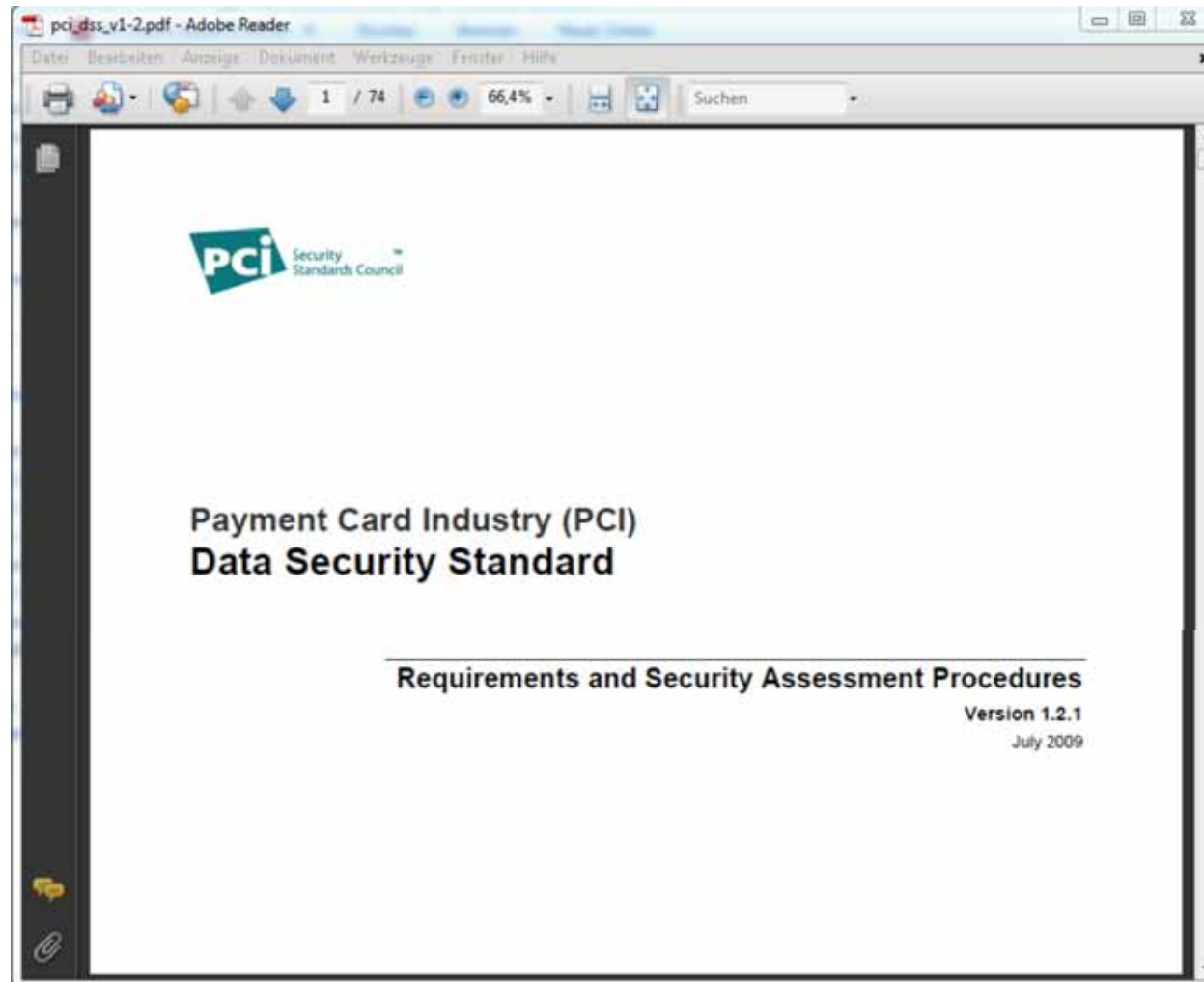


NO, we will not talk about this 😊



We will talk about this one

https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html



What is PCI

- **The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally.**
- **12 PCI DSS requirements for Security Assessment Procedures**



PCI Level for Merchant

- **PCI Compliance Level 1 - Merchants processing over 6 million Visa transactions annually (all channels) or Global merchants identified as Level 1 by any Visa region**
- **PCI Compliance Level 2 - Merchants processing 1 million to 6 million Visa transactions annually (all channels)**
- **PCI Compliance Level 3 - Merchants processing 20,000 to 1 million Visa e-commerce transactions annually**
- **PCI Compliance Level 4 - Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually**



PCI Level for Service Provider

- **Level 1 - VisaNet processors or any service provider that stores, processes and/or transmits over 300,000 transactions per year**
- **Level 2 - Any service provider that stores, processes and/or transmits less than 300,000 transactions per year**

Level*	Validation Action	Validated By
1	<ul style="list-style-type: none">• Annual On-Site PCI Data Security Assessment• Quarterly Network Scan	<ul style="list-style-type: none">• Qualified Security Assessor• Approved Scanning Vendor
2	<ul style="list-style-type: none">• Annual PCI Self-Assessment Questionnaire• Quarterly Network Scan	<ul style="list-style-type: none">• Service Provider• Approved Scanning Vendor



PCI Data Security Standard High-Level Overview



Build and Maintain a Secure Network

- Requirement 1: Install and maintain a firewall configuration to protect cardholder data
- Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Requirement 3: Protect stored cardholder data
- Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

- Requirement 5: Use and regularly update anti-virus software
- Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Requirement 7: Restrict access to cardholder data by business need-to-know
- Requirement 8: Assign a unique ID to each person with computer access
- Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Requirement 10: Track and monitor all access to network resources and cardholder data
- Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

- Requirement 12: Maintain a policy that addresses information security



Additional PCI DSS Requirements for Shared Hosting Providers

- A **hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS.**
- Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. **Each entity must comply with the PCI DSS** and validate compliance as applicable.




Third Parties/Outsourcing

- For service providers required to **undergo an annual onsite assessment, compliance validation must be performed on all system components where cardholder data is stored, processed, or transmitted.**
- A service provider or merchant may use a **third-party provider to store, process, or transmit cardholder data on their behalf, or to manage components such as routers, firewalls, databases, physical security, and/or servers. If so, there may be an impact on the security of the cardholder data environment.**
- For those **entities that outsource storage, processing, or transmission** of cardholder data to third-party service providers, the Report on Compliance (ROC) **must document the role of each service provider, clearly identifying which requirements apply to the reviewed entity and which apply to the service provider.**



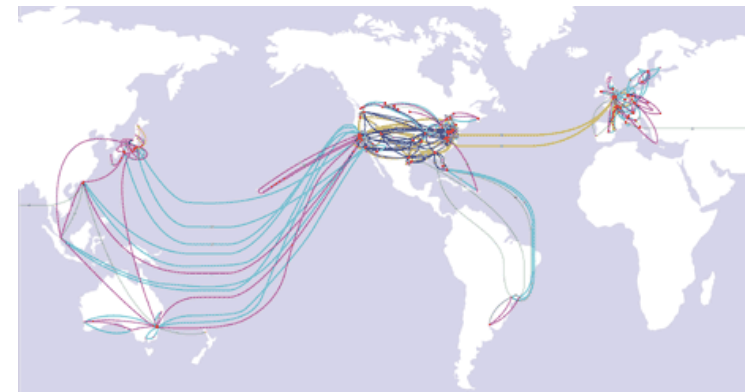
Isolation

- **Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of the corporate network is not a PCI DSS requirement.**
- **May reduce:**
 - The scope of the PCI DSS assessment
 - The cost of the PCI DSS assessment
 - The cost and difficulty of implementing and maintaining PCI DSS controls
 - The risk to an organization (reduced by consolidating cardholder data into fewer, more controlled locations)
- **Without adequate network segmentation (sometimes called a "flat network") the entire network is in scope of the PCI DSS assessment.**
- **QUESTION: Does a CLOUD-Provider isolate?** 



Details about Reviewed Environment

- **Include the following details in this section:**
 - A diagram of **each piece of the communication link**, including LAN, WAN or Internet
 - **List of hardware** and critical software in use **in the cardholder data environment**, along with description of function/use for each
 - List of service providers and other entities with which the company shares cardholder data
- **QUESTION: Do you know all affected connections / systems in the “CLOUD”?**



Compensating Controls

- **On an annual basis, any compensating controls must be documented, reviewed and validated by the assessor and included with the Report on Compliance submission.**



Is the cloud PCI ready?



Amazon EC2

referencing PCI requirement 12.8:

- If you're sharing cardholder information, i.e. credit card numbers, with a third party service provider, **you need to have a clause in your contract that makes the service provider responsible for the PCI compliance of their systems.**
- With the example given, Amazon's EC2, the chances of getting such a clause in your contract are almost non-existent.
- Therefore, if you're using Amazon's EC2, **you aren't going to be PCI compliant until such a time as Amazon makes a compliant infrastructure.** The same needs to be said of any of the other cloud vendor, it's not just EC2.

<http://www.mckeay.net/2008/11/02/pci-compliance-in-the-cloud-get-it-in-writing/>



Amazon EC2

<http://aws.amazon.com/agreement/>

- **We are not responsible for any unauthorized access to, alteration of, or the deletion, destruction, damage, loss or failure to store any of Your Content or other data which you submit or use in connection with your account or the Services.**
- **You are solely responsible for your Applications, including any data, text, images or content contained therein.**
- **You acknowledge that neither we nor our licensors are responsible in any manner, and you are solely responsible, for your Amazon S3 Content.**
- **You acknowledge that you bear sole responsibility for adequate security, protection and backup of Your Content and Applications. We strongly encourage you, where available and appropriate, to (a) use encryption technology to protect Your Content from unauthorized access, (b) routinely archive Your Content, and (c) keep your Applications or any software that you use or run with our Services current with the latest security patches or updates. We will have no liability to you for any unauthorized access or use, corruption, deletion, destruction or loss of any of Your Content or Applications.**
- **NEITHER WE NOR ANY OF OUR LICENSORS SHALL BE LIABLE TO YOU FOR ANY DIRECT , INDIRECT, INCIDENTAL , SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES , INCLUDING, BUT NOT LIMITED TO , DAMAGES FOR LOSS OF PROFITS , GOODWILL, USE , DATA OR OTHER LOSSES (EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES)**



It's all about risk – but you already know that 😊

- **If your service provider isn't willing to accept the risk associated with transferring, storing and manipulating cardholder data, you need a different service provider.**

PCI DSS Requirements	Testing Procedures
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.	12.8.2 Verify that the written agreement includes an acknowledgement by the service providers of their responsibility for securing cardholder data.



Let's get the party started

Hi,

Thank you for contacting Amazon Web Services. **Our payment system is PCI compliant** and it is an "alternative payment processing service" meaning your users re-direct to our platform to conduct the payment event using their credit cards or bank accounts. The benefit for you is that we handle all the sensitive customer data so you don't have to. If you haven't looked at it, I highly suggest you check out the features and functions of our Flexible Payment Service and our Payment Widgets (<http://aws.amazon.com/fps>).

As for PCI level 2 compliance, that requires external scanning via a 3rd party, PCI-approved vendor. It is possible for you to build a PCI level 2 compliant app in our AWS cloud using EC2 and S3, but you cannot achieve level 1 compliance. And you have to provide the appropriate encryption mechanisms and key management processes. If you have a data breach, you automatically need to become level 1 compliant which requires on-site auditing; that is something we cannot extend to our customers. **This seems like a risk that could challenge your business: as a best practice, I recommend businesses always plan for level 1 compliance. So, from a compliance and risk management perspective, we recommend that you do not store sensitive credit card payment information in our EC2/S3 system because it is not inherently PCI level 1 compliant. It is quite feasible for you to run your entire app in our cloud but keep the credit card data stored on your own local servers which are available for auditing, scanning, and on-site review at any time.**

Regards,

Cindy S.
Amazon Web Services
<http://aws.amazon.com>



But...

Hi,

Thanks for contacting us. I manage sales for AWS in the Southwest Region.

We are excited to hear about your interest in moving to EC2. We do not and will not provide a written agreement attesting compliance and assuming responsibility for cardholder data. Please see below for our general guidance on PCI compliance.

From a compliance and risk management perspective, we recommend customers not to store sensitive credit card payment information on EC2/S3 systems as they are not inherently PCI level 1 compliant. It is quite feasible one to run an entire application in AWS cloud while keeping the credit card data stored on within the local servers at the customer site, which are available for auditing, scanning, and on-site review at any time. As for PCI level 2 compliance, that requires external scanning via a 3rd party, PCI-approved vendor. It is possible for you to build a PCI level 2 compliant app in our AWS cloud using EC2 and S3.

Flexible Payment Service (FPS), which is AWS payment system is PCI compliant and it is an "alternative payment processing service" meaning a customer's users re-direct to our platform to conduct the payment event using their credit cards or bank accounts.

Let me know if you any follow-up questions.

Thanks, Taimur

Taimur Rashid

Account Manager

Amazon Web Services

E-mail: taimur@amazon.com

<http://aws.amazon.com>



- **Compliance with German BDSG (and comparable EU legislation) can – this is at least the prevailing opinion – achieved if**
 - There are detailed contracts.
 - Take care of countries where data is processed (e.g. Amazon “regions”)
 - Encrypt where operationally feasible
 - Deletion/wiping
- **Currently (most) public cloud offerings are not regarded suitable if SOX or PCI compliance are aimed for.**



- **Microsoft Azure Security Overview:**
 - <http://go.microsoft.com/?linkid=9740388>
- **Amazon AWS Security Overview:**
 - <http://aws.amazon.com/security/>
- **ISECOM Trust Metric**
 - www.packetstormsecurity.org/papers/presentations/Mastering_Trust_Sampler.pdf



■ Data Protection

- Geo-location properties in Windows Azure Portal
- Agreement for “Auftragsdatenverarbeitung” will be helpful
 - Not sure if they sign this though.

