Cloud Compliance and Privacy Protection

Cloud Strategy Partners, LLC

Sponsored by: IEEE Educational Activities and IEEE Cloud Computing
This IEEE Cloud Computing tutorial has been developed by Cloud Strategy Partners, LLC. Cloud Strategy Partners, LLC is an expert consultancy firm that specializes in Technology and Strategy relating to Cloud Computing.
In this tutorial, we will discuss cloud compliance standards including security controls and cloud infrastructure, NIST Cloud Compliance, CSA Cloud Compliance and Data Protection. Next we will review PCI DSS Cloud Computing Guidelines. We will also discuss Privacy Protection in Cloud and Big Data including CSA Top Ten Big Data Security and Privacy Challenges and US-EU Safe Harbor Framework.
Outline
In this Lesson we will cover:

- Compliance standards
  - Security Controls and Cloud infrastructure
  - NIST Cloud Compliance
  - CSA Cloud Compliance and Data Protection
- PCI DSS Cloud Computing Guidelines
- Privacy Protection in Cloud and Big Data
  - CSA Top Ten Big Data Security and Privacy Challenges
  - US-EU Safe Harbor Framework

Security and Compliance
Security and compliance are related and in some cases interchangeable

Security is commonly defined as a set of technical, physical, and administrative controls in order to ensure normal operation of a system or application

Security is often associated with the CIA triad Confidentiality, Integrity, Availability
Appropriate level of security requires organizations to take measures and comply to the numerous security controls

Compliance is a certification or confirmation that the system or an organization meets the requirements of specified standards, established legislation, regulatory guidelines or industry best practices that can be jointly defined as compliance framework

Why it is important for cloud? -When moving to cloud, the organization moves from internal security and operational environment/context (that may not be formally defined) to external operational security that will become a part of SLA (or business requirement) with CSP
As we will see, there are real challenges with achieving compliance for cloud based applications/solutions

General Regulatory Requirements for Cloud Compliance
General standards and recommendations

ISO/IEC 27001:2005 Certification on security infrastructure
Industry standard: the risk-based information security management program that follows a plan-do-check-act process. Service Organization Control SOC 1 (SSAE 16/ISAE 3402) and SOC 2 and 3 (AT 101)

SOC 2 is a detailed attestation report (often restricted) for service organizations that contain strict standards for security, availability, processing integrity, confidentiality, and privacy. SOC 3 is a general purpose report which summarizes the SOC 2 audit. A number of standards and Best Practices documents are addressing Cloud Security in general.

Cloud Security Alliance is an authoritative body with wide international membership that provides wide research and best practices collection in cloud security and currently also covering Big Data.

ENISA is a European body that is recognized for their research and activity on cyber infrastructure security with focus on risk and threats analysis.

Industry and Governmental Regulatory Requirements (USA)
Let us now summarize the most important Industry and Governmental Regulatory Requirements (for the USA)
• Service Organization Control SOC 1 (SSAE 16/ISAE 3402) and SOC 2 and 3 (AT 101)
• Sarbanes Oxley Act (SOX) also known as "Corporate and Auditing Accountability and Responsibility Act" set enhanced standards for all US public company boards, management and public accounting firms.
• HIPAA/HITECH -The U.S. Health Insurance Portability and Accountability Act (HIPAA) and HITECH (Health Information Technology for Economic and Clinical Health)
• The Federal Information Security Management Act of 2002 (FISMA)
• Department of Defense Information Certification Accreditation Process (DIACAP)
• Federal Risk and Authorization Management Program (FedRAMP)

Example: AWS Cloud Certification and Compliance
Because these are such important standards, Amazon has taken measures in AWS to meet these compliance profiles, as detailed in the slide. Microsoft Azure has done similarly.
Remember, just as there is a shared responsibility for Security on a cloud, between the Cloud Provider and the Cloud User, the same goes for compliance. Just because the Provider serves up a compliant platform does not mean the User application is automatically compliant.

Later in this tutorial we will walk through an example of the certification and compliance of AWS and Microsoft Azure clouds.

**Example: Microsoft Azure Certification and Compliance**

As mentioned in the previous slide, Microsoft has also taken strong efforts to make Microsoft Azure compliant with essentially the same profiles.

**Mapping Compliance and Cloud Infrastructure Components**

This illustrates relations between cloud based customer applications infrastructure and the main security controls applied to cloud infrastructure functional components. All this to comply with different security and other regulations. Compliance domains include:

- General Information Systems and IT regulations
- Government
- Finance
- Healthcare
- Energy

Application and infrastructure layers include

- Public/Private/Hybrid cloud infrastructure and/or platform provided by Cloud Service Providers
- Customer cloud based applications and infrastructure that may include multiple clouds and can treated as inter-cloud
- Enterprise or end user clients and IT infrastructure
The illustration in the slide also shows a number of security control or functionalities that work at different layers of the cloud based infrastructure.

Consistent security compliance can be achieved when combining all components and addressing at all layers.

Starting from strong cloud platform security supported by consistent security keys and session management that bind all security services/properties to platform security and integrity.

Continuing through applications security layer that includes network security, access control, policy management and data security. And finally, supported by corresponding security measures in enterprise IT infrastructure.

Security and Compliance Questions
The main questions that security and compliance auditors ask cloud service providers (on behalf of customers):
• Where is our data going to reside?
• Who is going to look after it?
• Who is going to be able to see it?
• Is it going to be the people that manage the infrastructure for us?
• Is it going to be internal and external people?
• And if we use a public cloud how secure is that cloud platform for us?
• Is the cloud going to be segregated from other organizations’ data?

NIST SP 800-53 Revision 4, Security and Privacy Controls
Now we will begin to review each of the important compliance profiles. First consider NIST SP 800-53. NIST SP 800-53r4 provides a catalog of security and privacy controls to protect organizational operations, organizational assets, individuals from a diverse set of threats including hostile cyber-attacks, natural disasters, structural failures, and human errors.
State-of-the-practice security controls have been developed addressing such areas as mobile and cloud computing; applications security; trustworthiness, assurance, and resiliency of information systems; insider threat; supply chain security; and the advanced persistent threat. Security controls are defined as the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Security controls are used to avoid, counteract or minimize security risks. Security control is an important concept in security design and security risk management. The NIST SP 800-53 Risk Management Framework defines the Security Life Cycle and includes 6 steps as detailed in the slide.

**Security Controls: Classes and Families**

Security controls described in SP800-53 Release 4 have a well-defined organization and structure. For ease of use in the security control selection and specification process, controls are organized into 18 families.

Each family contains security controls related to the general security topic of the family. A two-character identifier uniquely identifies security control families, for example, RA (Risk Assessment).

Security controls may involve aspects of policy, oversight, supervision, manual processes, actions by individuals, or automated mechanisms implemented by information systems/devices.

The security controls in the standard are organized into classes and families for ease of use in the control selection and specification process. There are three general classes of security controls (i.e., management, operational, and technical). Each family contains security controls related to the security function of the family. A two-character identifier is assigned to uniquely identify each control family. Table above summarizes the classes and families in the security control catalog and the associated family identifiers. The slide summarizes this in a Table.

**CSA3.0 Security Guidance for Critical Area of Focus in Cloud Computing**

The Cloud Security Alliance was formed to make sense out of the many compliance profiles, specifically in the context of Cloud Computing.
The document uses CSA Cloud Services Model that is used to map the security concerns to the cloud services and functional components in different cloud services models IaaS, PaaS, SaaS.

The CSA3.0 defines 13 domains of the security concerns for Cloud Computing that are divided into two broad categories that define corresponding security controls. The 13 are divided into Governance Domains and Operational Domains. These are listed in the Slide.

**CSA GRC Stack: Governance, Risk Management and Compliance**

The CSA provides a conceptual “Governance, Risk, and Compliance Stack” as a toolkit for enterprises, cloud providers, security solution providers, IT auditors and other stakeholders to assess both private and public clouds against industry established best practices, standards and critical compliance requirements.

Cloud Controls Matrix (CCM) is designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider.

Consensus Assessments Initiative Questionnaire (CAIQ) provides an industry-accepted way to document what security controls exist in IaaS, PaaS, and SaaS offerings, providing security control transparency.

The CSA has other initiatives as well: CloudAudit and Cloud Trust Protocol (CTP). The CSA also provides training course on the GRC Track and free version of Courseware.

**Jericho Forum’s Cloud Cube Model**

Another way of visualizing how combinations of cloud service models, deployment models, physical locations of resources, and attribution of management and ownership, is the Jericho Forum’s Cloud Cube Model.

The Cloud Cube Model illustrates the many permutations available in cloud offerings today and presents four criteria/dimensions in order to differentiate cloud “formations” from one another and the manner of their provision, in order to understand how cloud computing affects the way in which security might be approached.

The Cloud Cube Model also highlights the challenges of understanding and mapping cloud models to control frameworks and standards such as ISO/IEC 27002, which provides “...a
series of guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization.”

The ISO/IEC 27002, section 6.2, “External Parties” control objective states: “…the security of the organization’s information and information processing facilities should not be reduced by the introduction of external party products or services…”

CSA3.0: Mapping the Cloud Model to the Security Control & Compliance

The illustration in the slide shows an example of how a cloud service mapping can be compared against a catalogue of compensating controls to determine which controls exist and which do not—as provided by the consumer, the cloud service provider, or a third party. This can in turn be compared to a compliance framework or set of requirements such as PCI DSS, as shown.

It refers to 2 other general security services management standards
ISO/IEC 27002:2013 Code of Practice for InfoSec Controls

First, one classifies a cloud service against the cloud architecture model. Then it is possible to map its security architecture as well as business, regulatory, and other compliance requirements against it as a gap-analysis exercise. The result determines the general “security” posture of a service and how it relates to an asset’s assurance and protection requirements.

PCI DSS Principles and Requirements (Version 3.0, 2013)

PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. The standard is intended to help organizations proactively protect customer account data. PCI DSS defines a group of principles and accompanying requirements. These requirements are summarized in the Table in the slide.


PCI DSS applies to all kinds of computing infrastructures. Cloud infrastructures pose special challenges.
To address these cloud specific issues, a document called “Information Supplement: PCI DSS Cloud Computing Guidelines” was published in February 2013. It contains the following sections:

- **Cloud Overview** – provides explanation of common deployment and service models for cloud environments, including how implementations may vary within the different types.

- **Cloud Provider/Cloud Customer Relationships** – outlines different roles and responsibilities across the different cloud models and guidance on how to determine and document these responsibilities.

- **PCI DSS Considerations** – provides guidance and examples to help determine responsibilities for individual PCI DSS requirements, and includes segmentation and scoping considerations.

- **PCI DSS Compliance Challenges** - describes some of the challenges associated with validating PCI DSS compliance in a cloud environment.

- **Additional Security Considerations** – explores a number of business and technical security considerations for the use of cloud technologies.

---

**Audience: Involved Parties/Stakeholders**

For PCI DSS compliance, Cloud customers, cloud service providers and regulators must work together to determine the solutions that best meet the needs of stakeholders:

- **Merchants**: Enterprise and public sector cloud customers must be able to achieve their compliance obligations while using cloud services.
- **Individuals using the cloud** have an expectation that their personal information will be protected and used appropriately.

Cloud service providers must have clear mechanisms to evaluate and communicate capabilities.

- **Assessors**: Regulators and industry governing bodies need to have confidence that their requirements are met and verified.

---

**Example: Controls Assignment for Different Cloud Service Models (PCI DSS)**

Like all compliance profiles, PCI DSS assigns Controls as a mechanism to implement the compliance.
In Cloud Computing, because there are different service models (IaaS, PaaS, SaaS), in these different service models the controls may be the responsibility of the Provider, or of the User. The slide contains an illustration which shows how Controls assignments vary for different cloud service models.

**Example: PCI DSS Responsibilities Sharing**
The slide contains an illustration which shows how the responsibility sharing works for the different service models (IaaS, PaaS, SaaS), for the Provider, or of the User.

**Segmentation Considerations**
One of the key architectural notions of PCI DSS is about Segmentation, that is, isolating the parts of the computing infrastructure which have access to personal card information. Segmentation on a cloud based infrastructure must ensure similar level of segmentation as with physical infrastructure.

Mechanisms to ensure appropriate segmentation may be applied at the network, operating system and application layers. Cardholders data isolation must be ensured (Multi-tenant). Cloud environments must be isolated from each other.

Examples of correctly segmented cloud environments:
- Traditional Application Service Provider (ASP) model where physically separate servers are provided for each client's environment. Virtualized servers that are individually dedicated to a particular client, including any virtualized disks such as SAN, NAS or virtual database servers.
- Environments where clients run their applications in separate logical partitions using separate database management system images and do not share disk storage or other resources.

Examples of not correct segmentation:
- Environments are separated only by access control at the application or operating system level.

**Segmentation Technologies**
Different technologies are used to implement Segmentation:
- Physical firewalls and network segmentation at the infrastructure level.
- Firewalls at the hypervisor and VM level.
- VLAN tagging, in addition to firewalls.
- Intrusion prevention system.
• Data loss prevention tools at the hypervisor and/or VM level
• Controls to prevent out-of-band communications
• Isolation of shared processes and resources from client environments
• Segmented data storage for each client
• Strong, two-factor authentication
• Separation of duties and administrative oversight
• Continuous logging and monitoring of perimeter traffic

PCI DSS Compliance Challenges - Examples
Challenges arise when implementing PCI DSS. Example challenges are:

• Clients may have little or no visibility into the CSP’s underlying infrastructure and the related security controls.

• Clients may have limited or no oversight or control over cardholder data storage.

• Some virtual components do not have the same level of access control, logging, and monitoring as their physical counterparts.

• Perimeter boundaries between client environments can be fuzzy

• It can be challenging to verify who has access to cardholder data processed, transmitted, or stored in the cloud environment. Public cloud environments are usually designed to allow access from anywhere on the Internet.

• It can be challenging to collect, correlate, and/or archive all of the logs necessary to meet applicable PCI DSS requirements.

• It can be challenging for organizations to verify that cardholder card data has not “leaked” into the cloud.
Many large providers might not support right-to-audit for their clients. Clients should discuss their needs with the provider to determine how the CSP can provide assurance that required controls are in place.

What Does PCI DSS Compliance mean?
Cloud service validation for certain PCI DSS requirements does not automatically transfer to the client environments within the cloud service.
Client’s PCI DSS compliance does not result in any claim of compliance for the CSP, even if the client’s validation included elements of the service managed by the CSP.
In general, one party’s compliance doesn’t solve the overall compliance SLA and other written agreements should clearly delineate responsibility between parties.

PCI DSS compliance validation and testing (with associated controls and permissions) should be clearly detailed in SLA.

Privacy Protection in Cloud and Big Data
Modern cloud based applications (in particular those that are empowered with the Big Data technologies) collect a lot of different information about users - their behaviour and preferences - and can correlate it with other information.
This leads to special Privacy considerations.

Data Privacy Protection Regulation
To answer the Data Privacy concerns on Clouds and from Big Data, Security and compliance standards have emerged specifically covering data protection and privacy.

- The White House report ‘Big Data: Seizing Opportunities, preserving values’ (May 2014)

- Consumer Data Privacy In A Networked World: A Framework For Protecting Privacy And Promoting Innovation In The Global Digital Economy (February 2012)

- HIPAA/HITECH - The U.S. Health Insurance Portability and Accountability Act (HIPAA) and HITECH (Health Information Technology for Economic and Clinical Health). This Act was created by the US federal government include provisions to protect patients' private information.
• Protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.1.2012, COM(2012)

• U.S.-EU Safe Harbor Privacy Principles and Frequently Asked Questions (FAQs)

---

**Personal Privacy: Historical View**

One of the significant publications on big data privacy challenges is the White House report ‘Big Data: Seizing Opportunities, preserving values’ published in May 2014 (Executive Office of the President, 2014). The report is the result of the 90-day study commissioned by the President of the United States to examine how big data will transform the way people live and work and how big data will alter the relationships between government, citizens, businesses and consumers.

The report contains both a comprehensive overview of the data protection and privacy regulations in the United States in their historical development and high-level recommendations for how to address privacy issues in big data applications. The main approach in developing recommendations was to protect privacy while not hindering/restricting development of new technology for the benefit of the whole society.

The document also refers to the historically first article by Samuel Warren and Louis Brandeis in 1890 ‘The Right to Privacy’ related to personal privacy that noted: ‘[r]ecent inventions and business methods call attention to the next step which must be taken for the protection of the per-son, and for securing to the individual . . . the right ‘to be let alone’ . . . numerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the house-tops.’”


**White House report “Big Data: Seizing Opportunities, preserving values” (2014)**

One of the significant publications on big data privacy challenges is the White House report ‘Big Data: Seizing Opportunities, preserving values’ published in May 2014 (Executive Office of the President, 2014). The report is the result of the 90-day study commissioned by the President of the United States to examine how big data will transform the way people live and work and how big data will alter the relationships between government, citizens, businesses and consumers.
The report contains both a comprehensive overview of the data protection and privacy regulations in the United States in their historical development and high-level recommendations for how to address privacy issues in big data applications. The main approach in developing recommendations was to protect privacy while not hindering/restricting development of new technology for the benefit of the whole society. The report expresses the opinion that despite widely discussed needs for personal control of the collected e-commerce and social data, the practical use of such control is impractical due to the unmanageable volume of information and its variety. Instead, the advertisement companies and other organizational users of the personally Wide implementation of Cloud Computing provided a basis for developing big data technologies and data-centric and data-driven applications that in their own turn facilitate cloud technologies development. Data security and privacy challenges in Cloud Computing and big data have been a focus of numerous study groups initiated by different governmental bodies that produced several valuable reports.

The document also refers to the historically first article by Samuel Warren and Louis Brandeis in 1890 'The Right to Privacy' related to personal privacy that noted: '[r]ecent inventions and business methods call attention to the next step which must be taken for the protection of the per-son, and for securing to the individual . . . the right 'to be let alone’ . . . numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.’"


The report analyzed ‘harmful consequences that might result from automated personal data systems’ and recommended certain safeguards when using such information in computer systems (Report, 1973).

Those safeguards, commonly known today as the Fair Information Practice Principles (FIPPs), form the basis of modern data protection regulation (Executive Office of the President, 2014).

Consumer Data Privacy In A Networked World: Consumer Rights (2012)

There has been visibility all the way to the end consumer on Privacy issues. The US has issued recent documents developed by President Obama’s administration provide a foundation for the Right for Privacy in our Information society. A key document in this respect is the ‘Consumer Data Privacy In A Networked World: A Framework For
Protecting Privacy And Promoting Innovation In The Global Digital Economy’ published in February 2012, which states the following rights:

- **Individual Control**: Consumers have a right to exercise control over what personal data organizations collect from them and how they use it.

- **Transparency**: Consumers have a right to easily understandable information about privacy and security practices.

- **Respect for Context**: Consumers have a right to expect that organizations will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.

- **Security**: Consumers have a right to secure and responsible handling of personal data.

- **Access and Accuracy**: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data are inaccurate.

- **Focused Collection**: Consumers have a right to reasonable limits on the personal data that companies collect and retain.

- **Accountability**: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.

---

**EU Data Protection Regulation**

Europe has also been quite concerned about Data Protection and Privacy. The EU has established that:

Everyone has the right to the protection of personal data Under EU law, personal data can only be gathered legally under strict conditions, for a legitimate purpose. Furthermore, persons or organizations which collect and manage your personal information must protect it from misuse and must respect certain rights of the data owners which are guaranteed by EU law.

Privacy impact and requirements Right to be forgotten (RTBF) – complex issue for global cloud infrastructures and all information collected on the web and mobile applications. To support this, the EU documents outlining EU regulatory basis for data protection in cloud
Unleashing the Potential of Cloud Computing in Europe

Protection of individuals with regard to the processing of personal data and on the free movement of such data

US-EU “Safe Harbor” Framework

In order to bridge differences in approach and provide a streamlined means for U.S. organizations to comply with the EU Directive, the U.S. Department of Commerce in consultation with the European Commission developed a so-called “Safe Harbor” framework that defines key principles and provides recommendations for companies to protect personal data and personal information.

“Personal data” and “personal information” are data about an identified or identifiable individual that are recorded in any form.

7 Safe Harbor privacy principles

NOTICE: An organization must inform individuals about the purposes for which it collects and uses information about them, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure.

CHOICE: An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party(1) or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected.

ONWARD TRANSFER: To disclose information to a third party, organizations must apply the Notice and Choice Principles.

SECURITY: Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

DATA INTEGRITY: Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used.

ACCESS: Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete.

ENFORCEMENT: Effective privacy protection must include mechanisms for assuring compliance with the Principles, and consequences for the organization when the Principles are not followed.

CSA Top Ten Big Data Security and Privacy Challenges

Big Data motivate more detailed look at the data security and privacy protection challenges and suggested solutions which are applicable to general data protection in cloud taking into account that that due to scale of Big Data the Big Data applications are implemented in cloud and rely on cloud infrastructure and platform services.

CSA Top Ten are defined for the following functional components:

1 - Big Data sources that may include sensor, devices, large industrial objects as well as web, network and human
activity 2 –Data input and data provenance 3 –Data processing environment 4 –Cloud based Big Data infrastructure 5 –Data storage (cloud based) 6 –Data output and visualization
The slide contains an illustration which shows how these fit together.

CSA Top Ten Big Data Security Challenges by Functional Groups (1)
Generally, the Top Ten challenges can be grouped into four functional groups (but in fact they are more inter-related as illustrated in the next slide)
A. Infrastructure security
B. Access control and policy
C. Data Privacy and Confidentiality
D. Data Management

CSA Top Ten Big Data Security Challenges by Functional Groups (2)
This slide contains an illustration which shows the CSA Top Ten Big Data Security Challenges by Functional Groups

CSA Top Ten TT06. Scalable and Composable Privacy Preserving Data Mining and Analytics
One interesting CSA Top Ten concern to study is TT06. Scalable and Composable Privacy Preserving Data Mining and Analytics

This concern is regarding Big Data technologies and applications can potentially violate privacy and extract Personally Identifiable Information (PII) from data that initially has not been intended for this

In general, business use of Big Data analytics is well regulated by a number of privacy compliance standards and regulation acts that are applied at the discretion of companies. However, this may not prevent from intentional privacy violation by insider attacks when a worker that has access to the general data stores can access information not intended to him or her.

Solution and Implementation: Privacy-preserving analytics is an open and actively researched area.

Straightforward solution with encrypting data and potentially even using homomorphic encryption in the future will not solve all problems.
The right solution should include measures in multiple areas such as regulation, access control, data protection, accountability and provenance.

---

**CSA Top Ten TT07. Cryptographically Enforced Data-Centric Security**

Another interesting CSA Top Ten concern to study is TT07. Cryptographically Enforced Data-Centric Security

On-demand provisioned and distributed character of the Big Data infrastructure, especially if it is cloud based, make it practically unfeasible to achieve full protection of data at all infrastructure layers and during the whole data lifecycle, unless data remain encrypted all time.

Until recent time, before invention of the homomorphic encryption, the cryptographic methods used didn’t allow encrypted data to be processed. Data could be transferred and stored in encrypted form but they must be decrypted to be processed.

Although current homomorphic encryption systems have limited functionality in the sense of supported operations on data and processed data size, the promises of homomorphic encryption will impact academic and industry research for the near future. Newly developed cryptographic systems allows solving such issues with managing encrypted data as encrypted data comparison, subset queries and arbitrary conjunction of such queries

---

**Summary and Take Away**

This Lesson covered:

Cloud compliance provides a basis for wider cloud services adoption and inter-cloud integration. Cloud compliance provides a basis for risk assessment, SLA definition and decision making when moving services to cloud

Compliance is supported by numerous standards, legislation, regulatory guidelines and industry best practices that jointly define a compliance framework

Knowing major cloud compliance standards is necessary for correct cloud services, design, deployment and operation

PCI DSS Cloud Computing Guidelines provides invaluable source best practices information and practical recommendations for all categories of cloud specialists and practitioners.
Protection and Privacy in cloud is regulated by not less numerous group of standards and regulatory document.

Personal data protection is an important area of governmental and inter-governmental regulation. EU-US Safe Harbor Framework is one of such international frameworks.

Emerging Big Data technologies that are increasingly used by businesses and typically run on cloud platform create new challenges to data protection and privacy. At the same time Big Data create a powerful driver for Cloud Computing development as well as improving data protection and privacy.