Cloud Standards and Security

1 Introduction

We provide an overview of standards relevant for cloud computing security. Besides giving a brief summary of different standards, and explaining how they work, we also provide two maps which show the main characteristics of standards and in which use cases they become relevant for cloud customers.

This work is done in the context of the EU cloud strategy[1] issued in 2012 by the EC which calls for ENISA to support the EC in listing certification schemes and standards. This is an intermediate result which merely lists and provides an overview of standards relevant for cloud computing customers, from a security perspective. As part of the cloud strategy there is a much more elaborate activity which looks at many more standards, and also from other perspectives. The result of this work was published in 2013[2]. This report is ENISA's contribution to this work. The overview of standards was produced in collaboration with Antonio Ramos[3].

1.1 Target audience

This document is aimed at CIO's, architects in SMEs and government organizations who are procuring cloud services. It may be of interest also for industry experts and industry associations.

1.2 Scope

This document analyses a range of different cloud standards from a security and resilience perspective, for customers (an SME for example) adopting or using cloud computing services. Standards we discuss in this document include security standards, cloud computing standards, interoperability standards etc. This is not an exhaustive or complete list – there are hundreds of standards that could be (or become) relevant. Especially in the area of information security governance and risk management there is a flurry of initiatives aiming to customize existing information security management standards (like ISO270001) to fit better the situation of cloud computing service providers.

We skip technical standards on and below the transport layer (i.e. Ethernet, TCP/IP, TLS/SSL, HTTP, SMTP etc.), because these layers are very generic and also highly standardized. For the sake of brevity we also skip a range of cryptographic standards which are used for encrypting or authenticating messages or stored data (i.e. SHA-1, SHA-256, Blowfish, RSA, ECC).

1.3 Structure of this document

In Section 2 we provide an overview of the different technologies involved in the different types of cloud computing. In Section 3 we give an overview of the cloud standards and their main characteristics. In Section 4 we split the procurement lifecycle in 7 use cases and in Section 5 we introduce two types of standards maps: One map shows which standards address which technological areas, and other characteristics of standards (openness, adoption rate, et cetera). In the other map

[1] https://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy
[2] http://www.etsi.org/news-events/news/734-2013-12-press-release-report-on-cloud-computing-standards
[3] www.leetsecurity.com

we show which standards address which use cases. We conclude with some observations about gaps and overlaps.

2 Cloud service model

There are many different types of cloud services, each involving different types of technology and assets. We give an overview below – see Figure 1. We use this model later to indicate the application domain (which services, which assets) of a standard.

- **Infrastructure as a Service**: In IaaS the provider offers storage (virtual file systems) or computing resources (virtual CPUs), accessible online. Examples include Amazon's Elastic Compute Cloud, Google's Compute Engine, Amazon Simple Storage Service, Google Cloud Storage, Microsoft Windows Azure Storage, Rackspace, Dropbox, et cetera. Note that certain abstract storage services accessible via the web (WSDL, REST) could also be considered SaaS.
- **Platform as a Service:** In PaaS, the provider delivers a platform for customers to run applications on (often web applications). Often PaaS providers provide a software development tool to develop applications for the platform. Typical types of applications that run on these platforms are scripts (PHP, Python, e.g.) or byte code (Java servlets, C#). Examples include Google App engine, Microsoft Azure, Amazon Elastic Beanstalk, et cetera.
- **Software as a Service:** In SaaS, the provider delivers full-fledged software or application, via the internet. Applications range from email servers, email clients, document editors, or customer relationship management systems. SaaS services can often be accessed with a browser or a web services client.
- **Facilities:** Facilities are the basic IT resources which underlies all types of cloud services (IaaS, PaaS, and SaaS), network, housing, cooling, power.
- **Organisation**: Organisation are the human resources, the processes and the policies and procedures that maintain the facilities and support the delivery of services.

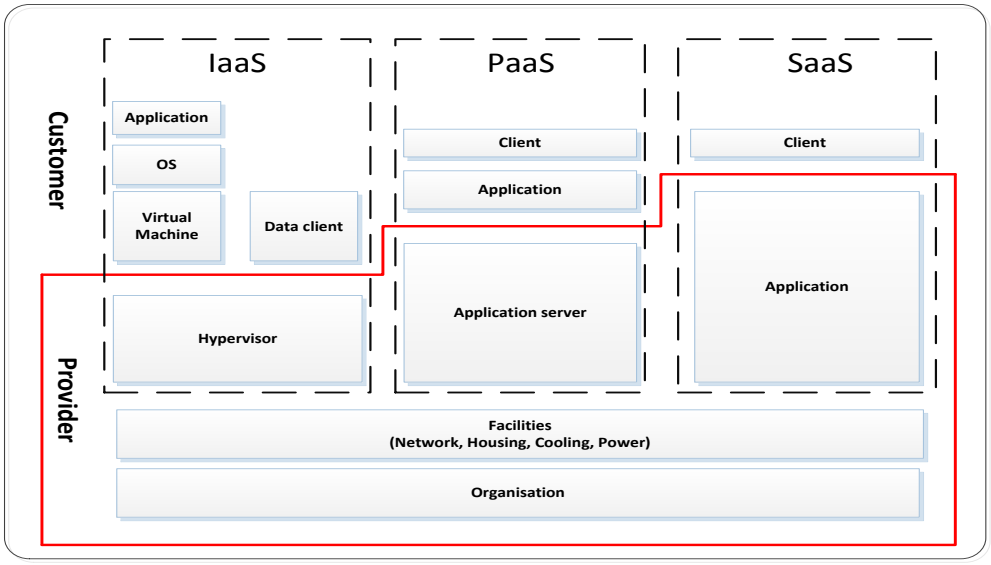

Figure 1 Map of different technologies in the different types of cloud services.

Note that some providers only offer IaaS or PaaS services, some providers only offer SaaS. It is not uncommon that SaaS providers run their applications on IaaS or PaaS providers[4].

3 Standards

In this document we focus on the following standards. This list is based on input from the ETSI working group on standards and the list of cloud standards published by NIST. We grouped closely related standards together for the sake of brevity.

1. HTML/XML
2. WSDL/SOAP
3. SAML/XACML
4. OAuth/OpenID
5. OData
6. OVF
7. OpenStack
8. CAMP
9. CIMI
10. ODCA – SuoM
11. SCAP
12. ISO 27001
13. ITIL
14. SOC
15. Tier Certification
16. CSA CCM

Note that it is a short list which is not exhaustive. There may well be other important standards or proposals interesting for discussion. The list of standards, with, per standard, a brief description of the standard, is included as an Annex A.

3.1 Characteristics of standards

For each standard we will look at some key characteristics. These characteristics are not intended as means of qualification. Below for example, we may say that a standard is used only by a limited number of organizations, or that a standard is not publicly available, but this does not mean that the standard is inferior nor that it is better, than other standards. Similar, we may say that a security standard is not specific for IaaS, but that does not mean that it is not a relevant security standard for an IaaS provider or customer.

3.1.1 Application domain

We indicate the type of assets addressed by the standard, based on the types of assets introduced in Section 2.

- Infrastructure as a Service
- Platform as a Service
- Software as a Service
- Facilities
- Organisation

For example, we denote that the application domain of a standard is IaaS, if the standard contains requirements for IaaS assets, such as virtual machines or hypervisors. Similarly, we denote that a

[4] A well-known example is Netflix (a video streaming site) which runs on Amazon AWS (computing services).

standard applies to Facilities if the standard contains requirements for setting up or maintaining facilities. Note that in the latter case the standard may be very relevant for cloud computing services, without being specific to one type of cloud service or the other.

3.1.2 Usage/Adoption

We indicate the estimate size of the user base, in terms of end-users or services. We use three levels:

- Globally (xxx) – thousands of organizations worldwide
- Widely (xx) - hundreds of organizations, regional or worldwide
- Limited (x) – tens of organizations or less, for example in pilots

3.1.3 Certification/auditing

We indicate whether or not there is a certification framework, to certify compliance with the standard, or, alternatively, whether or not it is common to have third-party audits to certify compliance. We use three levels:

- Common (xxx): Audits are common and certification frameworks exist.
- Sometimes (xx): Audits of compliance to the standard are sometimes carried out.
- Hardly (x): De-facto standard. There is no audit or certification asserting compliance.

3.1.4 Availability/Openness

We indicate whether or not the standard is public and open, in terms of access and in terms of the review process. We distinguish three levels:

- Fully open (xxx) - Open consultation for drafts (like W3C, IETF, OASIS, etc.), and open access to final versions (or for a small fee, less than 100 euro).
- Partially open (xx) - Consultation is closed/membership, but there is open access to the standard.
- Closed (x) – Consultations are not open to the public, and the standard is not public either (or there is a substantial fee, more than 100 euro).

3.2 Mapping standards and their characteristics

The characteristics can be used to make a map of the 16 standards. In Table 2 we show the application domain of the different standards, and the other characteristics (adoption, certification and openness).

	Application domain					Other characteristics		
	IaaS	Paas	Saas	Facilities	Organization	Usage/ Adoption	Certification/ Auditng	Openness/ Availability
HTML/XML	x		x			xxx	x	xxx
WSDL/SOAP	x		x			xxx	x	xxx
OAuth/OpenID			x			xxx	x	xxx
SAML			x			xxx	x	xxx
OData	x		x			x	x	xxx
OVF	x					xxx	x	xxx
OpenStack	x			x		xx	x	xx
CAMP		x				x	x	xx
CIMI	x					x	x	xxx
ODCA SUoM	x					x	x	xx
SCAP	x	x	x	x		xxx	x	xx
ISO 27001				x	x	xxx	xxx	xx
ITIL					x	xx	xxx	xx
SOC				x	x	xx	xxx	xx
Tier Certification				x		xx	xxx	x
CSA CCM				x	x	x	xxx	xxx

Table 1 Mapping the characteristics of the standards

4 Security and resilience perspective on cloud standards

In this section we provide a security and resilience perspective on the cloud standards, and particularly we show the standard(s) can help customers in mitigating security risks on the cloud services.

4.1 Procurement lifecycle

We split the overall procurement lifecycle in 7 high-level use cases – from the moment a customer wants to select a cloud service, until the customer exits the service contract and migrates out. The reason we split the procurement lifecycle in different parts is because in different parts of the procurement lifecycle, different cloud standards are important. In this section we detail the use cases. In the next section we discuss the relevance of cloud standards in each of the use cases.

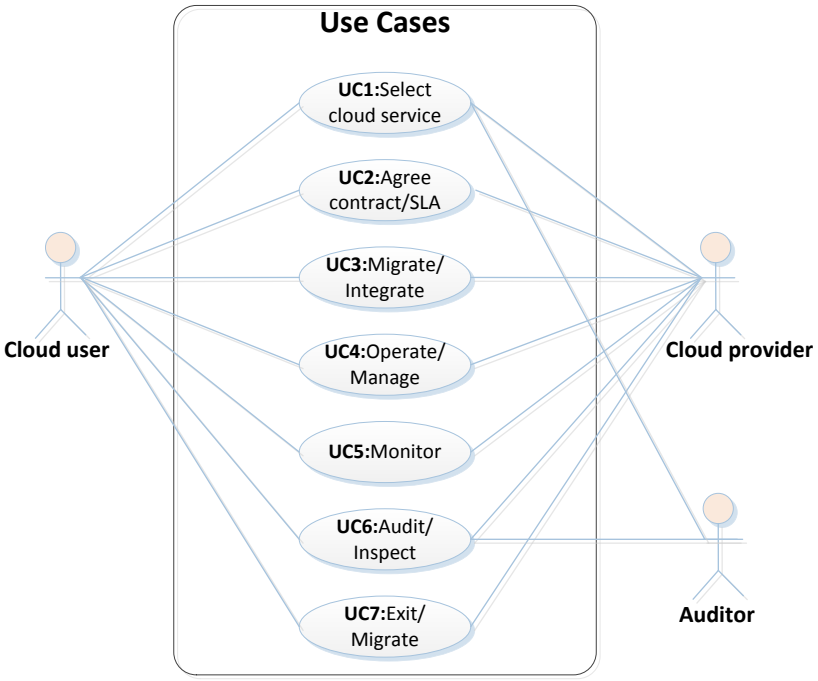

Figure 2 Business use case diagram with 7 high-level use cases.

UC1: Select cloud service: Customer wants to decide which cloud service to use (if at all). User could issue a request for proposal and compare offers, and/or carry out due-diligence on existing offers. Customer may require certification evidences for the provider or the service.

UC2: Agree contract/SLA: Customer wants to agree on a contract and a Service Level Agreement (SLA) defining detailed service levels and agreed procedures between the customer and the provider. Sometimes this involves negotiation, sometimes a checklist of options and a 'purchase' button.

UC3: Migrate/Integrate: Customer wants to migrate existing application and/or data to the cloud service or integrate the cloud service with existing services, systems or applications.

UC4: Operate/manage: Customer wants to operate and manage the cloud service.

UC5: Monitor: Customer wants to monitor the cloud service, during operation, for example to know about issues, service levels, etc.

UC6: Audit/Inspect: Customer wants to audit or inspect the cloud service, for example post-incident or to show compliance (as part of a compliance audit of the customer's organisation).

UC7: Exit/Migrate: Customer wants to exit the contract, and migrate its application and/or data out.

4.2 Security and resilience perspective

In this section we look at the different use cases and we explain per use case the security perspective and discuss which standards are particularly relevant in that use case, and how the standard(s) can help customers in mitigating risks for the security or resilience of the service. The Use Cases are grouped for brievity reasons (the standard characteristics are identical in these cases).

4.2.1 Selecting a cloud service, auditing and inspecting (UC1, UC6)

Security perspective

A key aspect of cloud computing is that the computing or storage resources are abstract, in the sense that the customer does not interact with, or knows about the detailed lower-level machinery used to deliver the computing resources, and often it is not directly apparent to the customer exactly how the computing resources are set up. For example, in SaaS a customer may be consuming a CRM solution, without interaction or knowledge of the underlying servers, architecture, network, or firewalls, used by the provider to deliver the CRM solution. The underlying resources may even be at another provider entirely. This is different from traditional IT deployments where the customer buys hardware, installs operating systems, firewalls, and finally the application. However, there are circumstances where a cloud computing customer needs to understand in more detail how the service is being delivered, and for example, which security processes or security measures are in place: when selecting a cloud service (UC1) or afterwards, when the customer needs to show compliance or following suspicion or an incident (UC6).

Existing standards

Information Security Management System (ISMS) standards, provide a fixed structure for organising, managing, and speaking security measures. ISMS standards are structured in several domains or areas ('risk management', 'human resources security', 'business continuity', et cetera). Each domain contains several lower level security objectives, named security controls or security processes ('continuous assessment of risks', 'raising security awareness with employees', 'preventing unauthorized access to premises'). Sometimes the standard also describes technical security measures that can be implemented to reach the security objectives ('implement a firewall', 'encrypt network traffic', 'have locks on doors').

- ISO27001/2 is the most well-known example of an information security management standard. ISO27001/2 is being used by a range of organisations, often in the private sector, including telecommunications providers, software development companies, but also construction companies, airline companies, banks, and so on. The standard is often used in the context of certification. In that case an independent auditor assesses compliance to the standard and a certification body (accredited by a national accreditation body) issues a certificate of compliance.
- CSA CCM is a list of controls, collected from a range of different international ISMS standards, such as ISO27001, PCI DSS, SOC2, and other. In this way CCM provides a framework for showing compliance to a range of different standards.
- SOC2 is a predefined set of security and privacy requirements. A SOC2 report could be used to provide customers an overview of security and privacy measures in place.

- The Tier standard is a set of requirements for security, protection and resilience measures for datacenters. A Tier 1, 2, or 3 certification can provide customers the assurance that the datacentre in question is resilient in the face of attacks or disasters.
- ITIL is a standard for managing service delivery. By asserting compliance to ITIL the provider can assure the customer that service delivery processes are set-up in a structured and predictable way.

4.2.2 Agree contract/SLA (UC2)

Security perspective

Like in outsourcing, also in cloud computing the formal agreement between customer and provider is crucial. In case of a conflict between customer and provider, both parties often fall back on what is formally agreed. The formal agreement between customer and provider is often called service contract. Without going into details about legalities, the contract can be split in three parts:

- The Service Agreement describes the type of service the provider commits to deliver. The service agreement describes the provider, the customer, who can be contacted when something goes wrong, the responsibilities for the provider, responsibilities for the customer, exceptions, which changes will be notified to the customer, if necessary technical details about functional requirements (what the service is supposed to do), the architecture of the service (how the service is set up), and non-functional requirements (such as security, quality of service, useability, logging etc).
- The Service Level Agreement [5] describes performance indicators or parameters, and the minimum values the provider commits to. The SLA often includes an up-time or availability percentage (99.9% or 99.99%) for some key functions, the performance of the service (or quality of service), the response time to incidents and issues, the time to fulfil certain service requests, and possibly other parameters of the service, such as the time to deploy patches, the time to replace parts, the time to notify incidents, et cetera.
- The Terms of Use describes how the customer should use the service and often what kind of usage is not allowed. The terms of service basically provides conditions to the service agreement, allowing the provider to forego its commitments or terminate the service in case the customer breaches the terms of use.

From a security perspective the service contract is important for the customer, not only because it formally commits the provider to implement certain security measures, but also because it formalizes who has which responsibilities when a security incident occurs, who is liable for which incidents, and if and the customer has the right to audit or inspect the security measures later on (for example, following an incident).

Existing standards

Like for other products and services, contracts and/or SLAs for cloud services are hardly standardized. The so-called 'fine-print' in contracts often hides important conditions and exceptions, and the terminology used in contracts or SLAs is often different from one provider to another. This means that customers have to read each contract and SLA in detail and sometimes consult a legal expert to understand clauses. Even if the customer has access to legal advice, it is often unpredictable how certain wordings in agreements will be interpreted in court. The standardization of IT services in cloud computing might enable further standardization of contracts and SLAs also. We mention one standard that defines specific standard service levels:

[5] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=6138

- SUoM is a standard developed by the Open Data Center Alliance, which describes a set of standard service parameters for IaaS, in 4 different levels (Bronze, Silver, Gold, Platinum), and covers among other things, security, availability, and elasticity.

4.2.3 Migration, integration and exit (UC3, UC7)

Security perspective

Interoperability and portability are not always seen as security properties. However, interoperability and portability can be crucial for a customer to mitigate certain security risks. For example, in case there is a legal conflict, the customer may need to move its data and processes to another provider – interoperability and portability are crucial in such cases to reduce down-time for the customer. Also in case of a disaster or a failure causing the service to be down for an extended period of time, a high degree of interoperability and operability can allow a customer to move data to other datacentres or to another provider. Interoperability and portability standards enable quicker integration and migration to a new service and it facilitates exit and termination of a service, as it allows a customer to quickly move to another provider.

Existing standards

Cloud computing services are much more standard than traditional IT deployments and most cloud computing services have highly interoperable (and standard) interfaces. We mention some key standards, which allow customers to move data and processes more easily to other providers or to fall back on back-up services:

- HTML / XML allow users to integrate different cloud services and to (more easily) migrate data from one provider to another.
- WSDL/SOAP is an interface standard (which uses XML) which enables interoperability between products and services, facilitating integration and migration. An emerging standard with similar purpose is
- OAuth/OpenID and SAML/XACML allows customers to integrate a cloud service with other (existing) IDM solutions, allowing easire integration of an identity provider with other (existing) websites (SaaS for example). OAuth/OpenID and SAML/XACML also facilitates portability between cloud implementations that support the framework.
- SAML/XACML provides users with an interface to manage the provision of identification and user authentication between user and provider.
- OData is a standard for accessing and managing data, based on JSON. OData allows customers to integrate a (IaaS or SaaS) cloud service with other (existing) services with cloud ones, making the integration of this kind of service easier.
- OVF is a standard format for virtual machines. OVF allows customers to use existing virtual machines, and move virtual machine images more easily from one provider to another.

4.2.4 Asset management and monitoring (UC4, UC5)

Security perspective

Asset management and monitoring are processes covered in the information security management standards discussed earlier. In the case of cloud computing, as mentioned already, many resources and assets are managed and monitored by the provider. Still the customers might need to manage some assets and resources – usually the more abstract and high-level assets and resources. Take for example PaaS, which allows customers to run applications on a platform. In this case, the provider will manage the lower-level assets (such as hardware, server operating systems, application services, et cetera), but the customer needs to manage the apps running on the platform. To take another

example, in SaaS for instance, the provider manages all assets from hardware up to and including the application, but in some cases customers still need to manage user accounts (provisioning, de-provisioning, etc).

In cloud computing managing resources and assets is one of the key administrative tasks of the customer, and this makes it particularly relevant also from a security perspective. Standards are important to allow customers to integrate asset management interfaces providers offer, with their own tools and systems, without the need for customization. This would make it also easier for customers to change providers, in case of issues (for example to mitigate lasting outages or legal disputes with a specific provider).

Existing standards

Particularly in IaaS and PaaS there are a number of standards for asset management and monitoring. We mention the key standards:

- OpenStack is a standard software stack for IaaS. OpenStack dashboard could be used also to monitor the usage of cloud resources and it provides a standard API for managing cloud resources.
- CAMP provides users with artifacts and APIs to manage the provision of resources of her PaaS provider. During the life of the service, CAMP supports the modification of PaaS resources, according to user needs.
- CIMI provides users with an interface to manage the provision of resources of her IaaS provider. During the life of the service, CIMI supports the modification of IaaS resources, according to user needs.
- SCAP is a standard for specifying vulnerabilities. SCAP allows customers to keep track of security flaws and evaluate the state of infrastructure in terms of vulnerabilities and patching.

4.3 Mapping standards to use cases

Table 1 summarizes this section and shows which standards are relevant for customers in the different use cases.

	UC1 (Select cloud service)	UC2 (Agree contract)	UC3 (Migrate/integrate)	UC4 (Operate/manage)	UC5 (Monitor)	UC6 (Audit/inspect)	UC7 (Exit/migrate)
HTML/XML			x				
WSDL/SOAP			x				
OAuth/OpenID			x	x			x
SAML/XACML			x	x			x
OData			x	x			x
OVF			x	x			x
OpenStack			x	x	x		
CAMP			x	x	x		x
CIMI			x	x			x
ODCA SUoM		x			x		
SCAP					x		
EuroPrise	x					x	
ISO 27001	x					x	
ITIL	x					x	
SOC	x					x	
Tier Certification	x					x	
CSA CCM	x					x	

Table 2 Use cases addressed by the standard.

5 Conclusions

In this document we listed 16 standards relevant for cloud computing customers, and we explained why they are relevant for customers from a security and resilience perspective. We have classified the standards according to their characteristics (in a map), and we have explained the relevance (from a security and resilience perspective) of these standards for customers, by looking at 7 use cases that span the cloud procurement lifecycle. We conclude with some general remarks.

During our research we found there are many cloud standards and cloud standards initiatives, many in experimental or draft stage. Some standards are aimed at very specific topics (for example, the structuring of data in user accounts), some standards are aimed at the entire cloud ecosystem (for example, supply chain security). Especially in the area of information security management system standards there is a flurry of initiatives, often paired with certification programs, often similar in scope, with a similar goal ("to increase trust in cloud providers") and often similar to the ISO27001 standard. It is interesting to see that most of these initiatives focus on rather generic requirements. What is usually out of scope are specific criteria, such as a minimum level of availability, minimum response times to incidents, a minimum set of functions for the administrative interfaces, or a minimum of liability or responsibility for security breaches. We believe that agreeing on more specific criteria could actually be very useful for customers, and we believe that standardization here could make it easier for customers to evaluate, compare and adopt cloud services. We also believe that it could be useful for the industry to focus less on standardizing the internal organization of information security management and more on the customer's security processes by providing standardized interfaces vis-à-vis those processes, so that customers can run these security processes more smoothly, hand-in-hand with the provider.

Data protection legislation is often mentioned as one of the key obstacles for customers in adopting to cloud computing. The borderless nature of cloud computing is puts the spotlight on the fact that that there are different jurisdictions with different data protection laws. We noted that there are hardly any standards that address the compliance needs of customers in this respect. Perhaps it is not really surprising that most information security standards do not address data protection compliance explicitly, simply because most data protection laws do not prescribe a specific set of security requirements either (stating simply that security should be 'appropriate'). Also, it is important to note here that there are different types of cloud services (such as IaaS and PaaS) which do not process or store personal data on their own. A service allowing customers to run virtual machines, for instance, might implement a set of generic security measures. It is up to the customer to decide what to do with the service – install a database of pet names, or install a health record application. Obviously in such cases, it is inappropriate to ask the cloud provider if the service is compliant to data protection legislation. The customer has the obligation to be compliant, while the provider can only explain the security measures it implements (for example, by referring to an information security standard).

While listing the standards we noted there are still hardly any standards for cloud SLAs and service contracts. This lack of standardisation complicates comparison of different services. For example, without a standard definition of uptime or availability it is difficult for customers to compare SLAs of different providers, or the performance of providers against these SLAs. At the same time, in cloud computing SLAs and contracts are very important for customers in managing their information security risks when adopting cloud services.

As mentioned earlier, cloud services are often more standard than legacy IT deployments. This creates important opportunities for security and resilience. We believe it is important that customers exploit these opportunities and we hope that this overview can help SMEs to understand how they can leverage existing cloud standards for mitigating security and resilience risks.

Annex A: List of standards

In this section we list the standards and describe them briefly.

A.1 HTML/XML

Full title	HyperText Markup Language (HTML) / eXtensible Markup Language (XML)
Description	**HTML** is the markup language for web pages – it is used for displaying text, links, images for human readers. HTML requires no further introduction. **XML** is a mark-up language and structure for encoding data in a format that is machine-readable. It is used for exchanging data between systems, for example in web services, but it is also used in application programming interfaces (APIs), or to store configuration files or other internal system data. Hundreds of XML-based languages have been developed, including RSS, Atom, SOAP, and XHTML. XML-based formats have become the default for many office-productivity tools. XML has also been employed as the base language for communication protocols, such as WSDL, and XMPP.
Link	W3C http://www.w3.org/html/ - http://www.w3.org/XML/ - HTML5 specs are developed by the WHAT WG http://www.whatwg.org/
Organisation	World Wide Web Consortium – the HTML WG and the XML Core WG. The latest HTML specifications have been developed by the WHATWG.
Application domain	**IaaS and SaaS** • XML allows exchange of data between applications (SaaS) and it provides a standard format for representing data which is used in plain storage service (IaaS).
Openness	Open - xxx • Development – Drafts are open to feedback and public comments. • Availability – Standards are freely available
Certification and compliance	No - x Compliance is often not formally certified. There are various schemes/tools that help in determining compliance (for example the W3C compliance validation checker, or XML editors that can validate XML documents).
Adoption	Globally – xxx Millions of companies use these standards, for external interfaces and internally to facilitate integration between products.

A.2 WSDL/SOAP

Full title	Web Services Description Language (WSDL)
Description	WSDL is an XML-based interface description language that is used for describing a web service. A WSDL description provides a machine-readable description of how the service can be called, what parameters it expects, and what data structures it returns. SOAP, an underlying standard, is used as a wrapper for transporting WSDL messages (for example over HTTP).
Link	http://www.w3.org/2000/xp/Group/
Organisation	World Wide Web Consortium : • XML Protocol Working Group; and • Web Services Description Working Group
Application domain	IaaS and SaaS WSDL allows integration of SaaS services – and WSDL is also used as standard for accessing data storage services (a type of IaaS).
Openness	Open - xxx: • Development – Discussion between W3C members (and potentially, non-members experts invited by the Group Chair). • Availability – Documents are freely available to download from XML Protocol /Web Service Description Working Groups
Certification and compliance	None - x Companies often implement WSDL on a voluntary basis, without any formal process to check compliance (such as certification). There are tools to validate interoperability and vendors sometimes participate in multi-vendor interoperability workshops.
Adoption	Globally – xxx Thousands of companies use WSDL.

A.3 OAuth/OpenID

Full title	OAuth 2.0 Authorization Framework
Description	OAuth is a protocol and language for expressing authorizations (to access data or service) and to exchange these authorizations between different websites. OpenID an online authentication protocol is a widely used authentication protocol which is part of OAuth. OpenID allows to integrate website (SaaS) with identity providers (SaaS). OAuth/OpenID is becoming the de-fact authN/auhtZ protocol standard in social networks. SAML/XACML is an alternative used widely in enterprise software and e-government, for example.
Link	http://tools.ietf.org/html/rfc6749
Organisation	Internet Engineering Task Force (IETF)
Application domain	SaaS • OAuth/OpenID standardizes authentication and authorisation protocols between identity providers (SaaS) and websites (SaaS).

Openness	Open - xxx • Development – Standard is discussed by IETF OAuth Working Group experts. • Availability – Document is freely available to download from IETF website.
Certification and compliance	None - x OAuth/OpenID is a de-facto standard and no formal certification of compliance is used. Multi-vendor interoperability workshops are sometimes organized.
Adoption	Globally – xxx Several large websites (Facebook, Google, et cetera), OAuth/OpenID and thousands of websites and applications – enabling SSO for millions of users.

A.4 SAML/XACML

Full title	Security Assertion Markup Language (SAML), Extensible Access Control Markup Language (XACML)
Description	SAML/XACML are XML-based languages and protocols for authentication and authorisation (on the web and inside local networks) of users for accessing websites. SAML/XACML supports the integration of websites and intranet servers with authentication/authorisation services and products, providing SSO for users (aka federation). SAML/XACML is used widely in enterprise software and e-government, for example. OAuth/OpenID are alternatives more widely used in social media.
Link	http://saml.xml.org/wiki/saml-wiki-knowledgebase
Organisation	Organization for the Advancement of Structured Information Standards (OASIS)
Application domain	SaaS As a framework that allows to access to an HTTP service, it works on the API/GUI component of the cloud service model.
Openness	Open - xxx • Development – Standard is discussed by OASIS Security Services Technical Committee experts. • Availability – Document is freely available to download from OASIS website.
Certification and compliance	None - x Compliance to SAML and XACML is usually not formally audited or certified – there are multi-vendor interoperability workshops.
Adoption	Globally – xxx Thousands of applications use or support SAML, but it is estimated than only less of 10% of the available applications (in fact, it is being replaced by Oauth as standard de-factor for identity management)

A.5 OData

Full title	Open Data Protocol
Link	http://www.odata.org/
Organisation	Microsoft developed the standard. It has been proposed for adoption by Organization for the Advancement of Structured Information Standards (OASIS)
Description	OData is a web protocol for querying and updating data. OData applies and builds upon Web technologies such as HTTP, Atom Publishing Protocol and JSON to provide access to information from a variety of applications, services, and stores.OData can be used to expose and access information from a variety of sources including, but not limited to, relational databases, file systems, content management systems and traditional Web sites.
Application domain	IaaS and SaaS - OData provides a (REST-full) API for managing data.
Openness/availability	xxx - Open: • Development – Standard is open for discussion/feedback via the OASIS OData Technical Committee. • Availability – Document is freely available to download from OData website.
Certification/auditing	None - x No formal audits or certification scheme for compliance.
Adoption/usage	Limited – x Tens of applications and tens of live services implement OData Protocol at the moment of issuing this report (according to OData website).

A.6 OVF

Full title	Open Virtualization Format
Link	http://www.dmtf.org/standards/ovf
Organisation	Distributed Management Task Force (DMTF)
Description	OVF is an open standard for packaging and distributing virtual machine images, independent of a particular hypervisor or processor architecture”.
Application domain	IaaS. - OVF is a format for packaging virtual machine images.
Openness/Availability	Open: • Development – Standard is discussed by DMTF group experts. • Availability – Document is freely available to download from DMTF website
Certification/auditing	OVF is a voluntary standard and there is no formal certification or auditing scheme for asserting compliance.
Adoption/usage	Globally – OVF has been adopted by major virtualization players, so thousands of users are using the standard.

A.7 OpenStack

Full title	OpenStack Open Source Cloud Computing Software

Link	http://www.openstack.org/
Organisation	OpenStack Foundation
Description	OpenStack is a free open source software for creating and running a cloud computing service on standard hardware. OpenStack covers the following services: compute, object storage, image service, identity, dashboard, networking, block storage, metering, and orchestration & service definition.
Application domain	IaaS, PaaS. – OpenStack standardizes the hypervisor.
Openness	Partly open: • Development – Software new functionalities are discussed between OpenStack Foundation experts. • Availability – Documents and source code are freely available to download from OpenStack website.
Certification and compliance	OpenStack is a voluntary standard, and there is no formal auditing or certification scheme to assert compliance.
Adoption	Widely – Hundreds of companies have joined the OpenStack project and/or are using OpenStack.

A.8 CAMP

Full title	Cloud Application Management for Platforms
Link	http://cloudspecs.org/CAMP/CAMP_v1-0.pdf
Organisation	Alliance (CloudBees, Cloudsoft, Huawei, Oracle, Rackspace, Red Hat, and Software AG)
Description	The main objective of CAMP is to leverage similarities between different PaaS offerings (using languages as Java, Python, and Ruby and frameworks such as Spring and Rails) and to produce a generic application and platform management API that is language, framework, and platform neutral. The specification includes the artifacts and APIs that need to be offered by a PaaS cloud to manage the building, running, administration, monitoring and patching of applications in the cloud contributing to the interoperability among self-service interfaces to PaaS clouds.
Application domain	PaaS - CAMP is a standard for managing (multiple) applications running on a PaaS infrastructure.
Openness	Partly open: • Development – Specification has been created by the organisations mentioned above. • Availability – Document is freely available to download from the CAMP website.
Certification/auditing	CAMP is a voluntary standard. There is no formal auditing or certification scheme to assert compliance.
Adoption/usage	Limited – Apart from founders some other organisations are adopting it.

A.9 CIMI

Full title	Cloud Infrastructure Management Interface (CIMI) Model and RESTful HTTP-based Protocol. An interface for managing cloud infrastructure.
Link	http://dmtf.org/sites/default/files/standards/documents/DSP0263_1.0.0.pdf
Organisation	Distributed Management Task Force, Inc. (DMTF)
Description	CIMI defines a logical model for the management of resources in IaaS. In CIMI basic resources of IaaS (machines, storage, and networks) can be managed using a REST-full protocol (over HTTP), with messages in JSON or XML. Open Virtualization Format (OVF) support in CIMI allows an OVF package to be used to create CIMI management resources by importing the package.
Application domain	IaaS - CIMI provides an interface for managing IaaS.
Openness	Open: • Development – Standard is discussed by DMTF Cloud Management Working Group experts. • Availability – Document is freely available to download from DMTF website.
Certification and compliance	None - CIMI is voluntary and there is no formal auditing or certification scheme to assert compliance.
Adoption	Limited – Tens of companies has publicly shown its support to CIMI since it was published in August, 2012.

A.10 ODCA – SUoM

Full title	Standard Units of Measure for IaaS
Link	http://www.opendatacenteralliance.org/document-sections/category/71-docs?download=458:standard_units_of_measure
Organisation	Open Data Center Alliance (ODCA)
Description	SUoM specifies quantitative and qualitative attributes of services to enable easier, more precise comparison between vendors. Metrics are either “quantitative” on a like-for-like basis (e.g., quantity of consumption, period of usage, etc.) or “qualitative” on a set of service assurance attributes (e.g., degree of elasticity, degree of service level, etc.).
Application domain	IaaS - The document includes units of measure for IaaS resources.
Openness/availability	Partly open: • Development – Standard is discussed by ODCA experts. • Availability – Document is freely available to download from ODCA website.
Certification/auditing	Standard Units of Measure for IaaS standard is voluntary and there is no body responsible to accredit in any way that a service is compliance with it.
Adoption/usage	Limited – Tens of organisations adhered to ODCA adhere to this document.

A.11 SCAP

Full title	Security Content Automation Protocol (SCAP)
Link	http://scap.nist.gov/ http://csrc.nist.gov/publications/nistpubs/800-126/sp800-126.pdf
Organisation	National Institute of Standards and Technology (NIST)
Description	SCAP is a suite of specifications that standardize the format and nomenclature by which software flaw and security configuration information is communicated, both to machines and humans. CVSS and CVE are the most well-known parts of SCAP. SCAP v1.2 contains eleven specifications: • Extensible Configuration Checklist Description Format (XCCDF), Open Vulnerability and Assessment Language (OVAL®), and Open Checklist Interactive Language (OCIL™). • Asset Reporting Format (ARF) and Asset Identification. • Common Platform Enumeration (CPE™), Common Configuration Enumeration (CCE™), and Common Vulnerabilities and Exposures (CVE®). • Common Vulnerability Scoring System (CVSS) and Common Configuration Scoring Systems (CCSS). • Trust Model for Security Automation Data (TMSAD).
Application domain	Facilities, IaaS, PaaS, and SaaS. The document tries to make easier the security interchange information between parties, at all levels with potential vulneratibilies, i.e. all the layers in the Cloud Model except organisation.
Openness	Partly open: • Development – Standard is discussed by NIST community. • Availability – Document is freely available to download from NIST website.
Certification and compliance	NIST provides an SCAP Content Validation Tool that organizations can use to help validate the correctness of their SCAP content.
Adoption	Some pieces of SCAP are *globally* adopted as CVSS or CVE, while the rest should be considered in limited use (CPE, CCE…). In fact, there are 43 content producers products that have been validated to be SCAP-compliant that correspond to the main vulnerability assessment vendors, so hundred of thousands of companies are consuming information SCAP-compliant.

A.12 ISO 27001

Full title	Information technology – Security techniques – Information security management systems - Requirements
Link	http://www.iso.org/iso/catalogue_detail?csnumber=42103
Organisation	International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)

Description	ISO/IEC 27001:2005 set the principles to define, develop and operate an Information Security Management System (ISMS) that could be certified afterwards for an accreditation body. It is based on the PDCA (plan-do-check-act) model fostering continuous improvement of information security, but it does not prescribe neither obliges to any kind of specific or security measures.
Application domain	Facilities and Organisation – ISO27K1 is a standard for information security management and is not specific for cloud services or a specific type of cloud service.
Openness/availability	Partly open: • Development of standard is discussed only by ISO/IEC . • Availability: Document is available for purchase from the ISO online store.
Certification/auditing	Standard is certifiable by accredited certification entities
Adoption/usage	Globally – Thousands of companies are certified against this standard (7.940 according to www.iso27001certificates.com, which cannot be consider a complete register)

A.13 ITIL

Full title	Information Technology Infrastructure Library
Link	http://www.itil-officialsite.com/
Organisation	UK's Cabinet Office.
Description	ITIL[6] is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business. ITIL describes processes, procedures, tasks and checklists that could be used by a service provider for establishing integration with the organization's strategy. It allows the organization to establish a baseline from which it can plan, implement, and measure. ITIL 2011 has five core publications: ITIL Service Strategy ITIL Service Design ITIL Service Transition ITIL Service Operation ITIL Continual Service Improvement
Application domain	Organisation. Due to the focus of this framework on service management, it has been considered that the element of the cloud model more affected by it is the organization one.
Openness	Partly open: Development of standard is discussed only by Cabinet Office . Availability: Document is available for purchase from the Best Management Practice online store.

[6] Based on Wikipedia definition, http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library

Certification and compliance	Certification could by achieved against ISO/IEC 20000:2 (IT Service Management Certification Scheme).
Adoption	Widely – Hundreds of companies are certified against ISO/IEC 2000 (713 according to http://www.isoiec20000certification.com, which cannot be consider a complete register)

A.14 SOC

Full title	Service Organization Control Reports
Link	http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/sorhome.aspx
Organisation	AICPA – American Institute of Certified Public Accountants CICA – Canadian Institute of Chartered Accountants
Description	SOC reports are internal control reports on the service provided by a service organization providing information that users need to assess the risks. These reports are the successors of famous SAS70 ones. These reports provides with an independent evaluation of the effectiveness of controls that address operations and compliance. In fact, there are three reporting options: SOC 1 (restricted use): Focus solely on controls at a service organization that are likely to be relevant to an audit of a user entity's financial statements. SOC 2 (generally restricted use): Uses the predefined criteria in *Trust Services Principles, Criteria and Illustrations* (security, availability, processing integrity, confidentiality and privacy) to provide a description of the service organization's system, auditor's tests of controls and results and auditor's opinion on that description. SOC 3 (general use – with a public seal): Uses the mentioned criteria to only provide auditor's opinion on whether the system achieved the trust services criteria.
Application domain	Facilities and Organisation. Requirements included in the *Trust Services Principles, Criteria, and Illustrations* are set in a generic way, i.e. although they affect every layer of the infrastructure, they are not specific for any layer.
Openness	Partly open: Development – Elaborated by AICPA/CICA experts Availability – Basic documents are freely available to download from AICPA and Webtrust.org websites; more specific ones have to be purchased.
Certification and compliance	SOC reports can be issued by independent Certified Public Accountants (CPAs) acting according to AICPA/CICA standards.
Adoption	Widely adopted – Hundreds of companies have been audited against this type of reports (previously known as SAS70 reports).

A.15 Tier Certification

Full title	Data Center Site Infrastructure Tier Standard
Link	http://uptimeinstitute.com/publications

Organisation	The Uptime Institute
Description	The standard is an objective basis for comparing the functionality, capacities, and relative cost of a particular site infrastructure design topology against others, or to compare group of sites.
Application domain	Facilities. The standard applies to the elements included in data centers: Hardware, housing and power/cooling.
Openness/availability	Not open: • Development – Elaborated and discussed by the Owners Advisory Committee (those organizations that have successfully achieved Tier Certification). • Availability – It is not available for download from Uptime Institute website; neither it is available for purchase.
Certification/audits	The Uptime Institute has retained the exclusive legal right to review, assess, and Certify data centers to the Institute's Tier Classification System. There are three steps: • Design Certification • Constructed Facility Certification • Operational Sustainability Rating
Adoption/usage	Widely adopted – There are 269 data centers certified from Tier II to Tier IV (according to Uptime Institute website).

A.16 CSA CCM

Full title	Cloud Controls Matrix v1.3 (CCM)
Link	https://cloudsecurityalliance.org/research/ccm/
Organisation	Cloud Security Alliance – CSA
Description	CCM collects and customizes security controls from other standards (ISO 27002, ISACA COBIT, PCI, NIST…), with a focus cloud computing services.
Application domain	Facilities and Organisation. Requirements included in the *CCM* are set in a generic way, i.e. although they affect every layer of the infrastructure, they are not specific for IaaS, PaaS or SaaS.
Openness	Open: • Development – Standard is discussed by CSA experts. • Availability – Document is freely available to download from CSA website.
Certification and compliance	The Open Certification Framework is a program that certifies or asserts compliance against CCM. OCM has three levels of assessment: • Self-assessment by the provider, publishing the way she complies with it using the Consensus Assessments Initiative Questionnaire (CAIQ) and the public Security, Trust & Assurance Registry (STAR). • Certification by a third party via CSA – Open Certification Framework. • Continuous monitoring is under development.

Adoption	Widely –Tens of organizations are registered in the STAR registry and hundreds of organizations use it.