Centro Studi

Process Development & Applied Research

gruppo orizzonti holding

Analysis of ISO 27001:2013 Controls effectiveness for Cloud Computing

Muhammad Imran Tariq
Vito Santarcangelo

ICISSP 2016
2nd International Conference on Information Systems Security and Privacy
Rome, Italy | 19 - 21 February, 2016

TOPIC

Cloud Computing provides a scalable, high availability and low cost services over the Internet. The advent of newer technologies introduces **new risks and threats** as well. Although the cloud has a very advanced structures and expansion of services, **security and privacy** concerns have been creating obstacles for the enterprise to entirely shift to the cloud.

MOTIVATION

Both **service providers and clients** should build an **information security system** and trust relationship with each other.

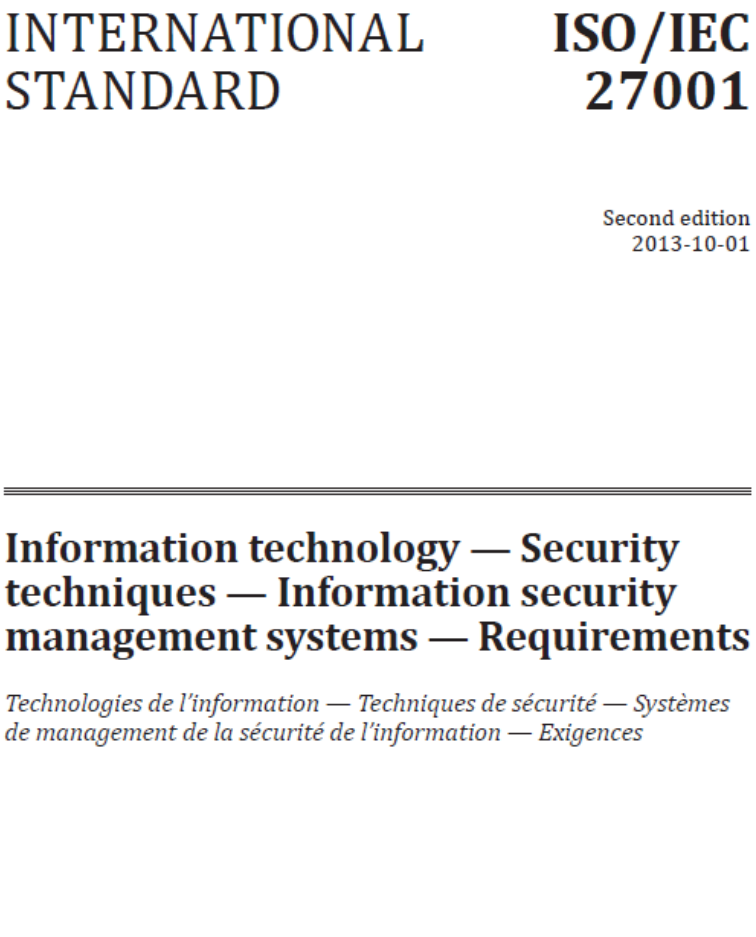
SCOPE OF THE WORK

In this research paper, we analyzed most widely used international and industry standard (**ISO/IEC 27001:2013**) for information security to know its **effectiveness for Cloud Organizations**, each control importance factor for on-premises, IaaS, PaaS and SaaS, and identify the most suitable controls for the development of **SLA** based Information Security Metrics for each Cloud Service Model.

1

ISO 27001:2013

Let’s start with the international standard for information security



ISO 27000 : Fundamentals and vocabulary

ISO 27001 : ISMS Requirements (normative)

ISO 27002 : ISMS Code of practice (guide)

ISO 27001's Annex A

list of 114 controls /best practices

(35 control objectives, 14 key points from A.5 to A.18)

ANNEX A

A.5 Information security policies – controls on how the policies are written and reviewed
A.6 Organization of information security – controls on how the responsibilities are assigned; also includes the controls for mobile devices and teleworking
A.7 Human resources security – controls prior to employment, during, and after the employment
A.8 Asset management – controls related to inventory of assets and acceptable use, also for information classification and media handling
A.9 Access control – controls for Access control policy, user access management, system and application access control, and user responsibilities
A.10 Cryptography – controls related to encryption and key management
A.11 Physical and environmental security – controls defining secure areas, entry controls, protection against threats, equipment security, secure disposal, clear desk and clear screen policy, etc.

ANNEX A

A.12 Operational security – lots of controls related to management of IT production: change management, capacity management, malware, backup, logging, monitoring, installation, vulnerabilities, etc.
A.13 Communications security – controls related to network security, segregation, network services, transfer of information, messaging, etc.
A.14 System acquisition, development and maintenance – controls defining security requirements and security in development and support processes
A.15 Supplier relationships – controls on what to include in agreements, and how to monitor the suppliers

ANNEX A

A.16 Information security incident management – controls for reporting events and weaknesses, defining responsibilities, response procedures, and collection of evidence

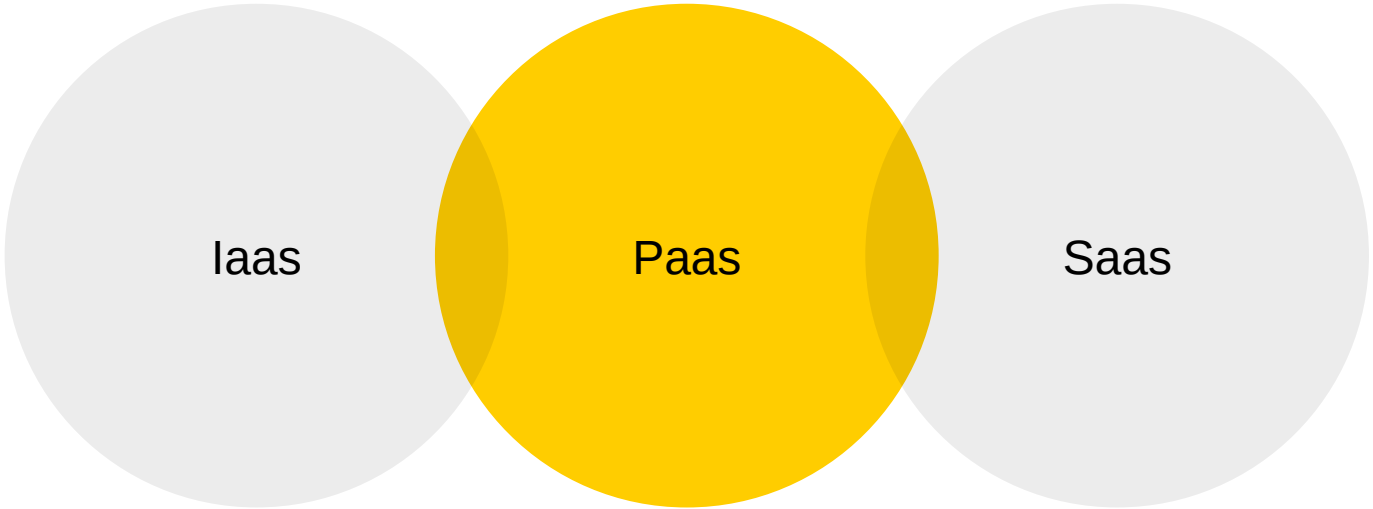
A.17 Information security aspects of business continuity management – controls requiring the planning of business continuity, procedures, verification and reviewing, and IT redundancy

A.18 Compliance – controls requiring the identification of applicable laws and regulations, intellectual property protection, personal data protection, and reviews of information security

2

CLOUD COMPUTING

CLOUD SERVICE MODELS



On premise (In House)

Executed by CSP

Executed by cloud customers

Comparison between Private and Public Cloud Service Models (Clayton, 2011).

Big concept

Evaluate effectiveness and importance of ISO/IEC 27001 controls for cloud computing

ISO 27001 AND CSP

Organization	Security Compliance
Amazon	SOC 1, SOC 2, SSAE 16, ISAE 3402, FISMA, DIACAP, FedRAMP, PCI DSS Level 1, ISO 27001, FIPS 140-2, HIPPA, CSA and MPAA
Salesforce	ISO 27001, SysTrust, SAS and 70 Type II
Microsoft	FISMA, PCI DSS, HIPAA, SOX, ISO 27001, SAS 70 TYPE 1 and II and NIST SP 800-53
Google	SAS 70 Type II, FISMA, ISO 27001 and NIST SP 800-53
IBM	FISMA, SAS 70 Type II, ISO 27001-2002, SSAE 16, SOC 2, NIST SP 800-53 and HIPPA

CSPs Security Certification and Accreditation

ISO 27001 Controls Evaluation Criteria

CRITERIA 1

- How much Control is effective for cloud development and service models (SaaS, PaaS and IaaS)?.

CRITERIA 2

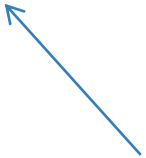
Suitable to be included in the SLA for Cloud?

Importance Factor Value	Importance Factor Description	Remarks
-	Irrelevant	Not relevant to Cloud Computing
1	Minimal	All Responsibilities are transferred to CSP
2	Moderately important	Major responsibilities are transferred to CSP
3	Important and relevant	Partially responsibilities are transferred to CSP
4	Highly important	Minor Responsibility transferred to CSP
5	Highest importance	Cloud customer and CSPare responsible to manage their own Cloud.

ISO 27001 Controls Evaluation Criteria

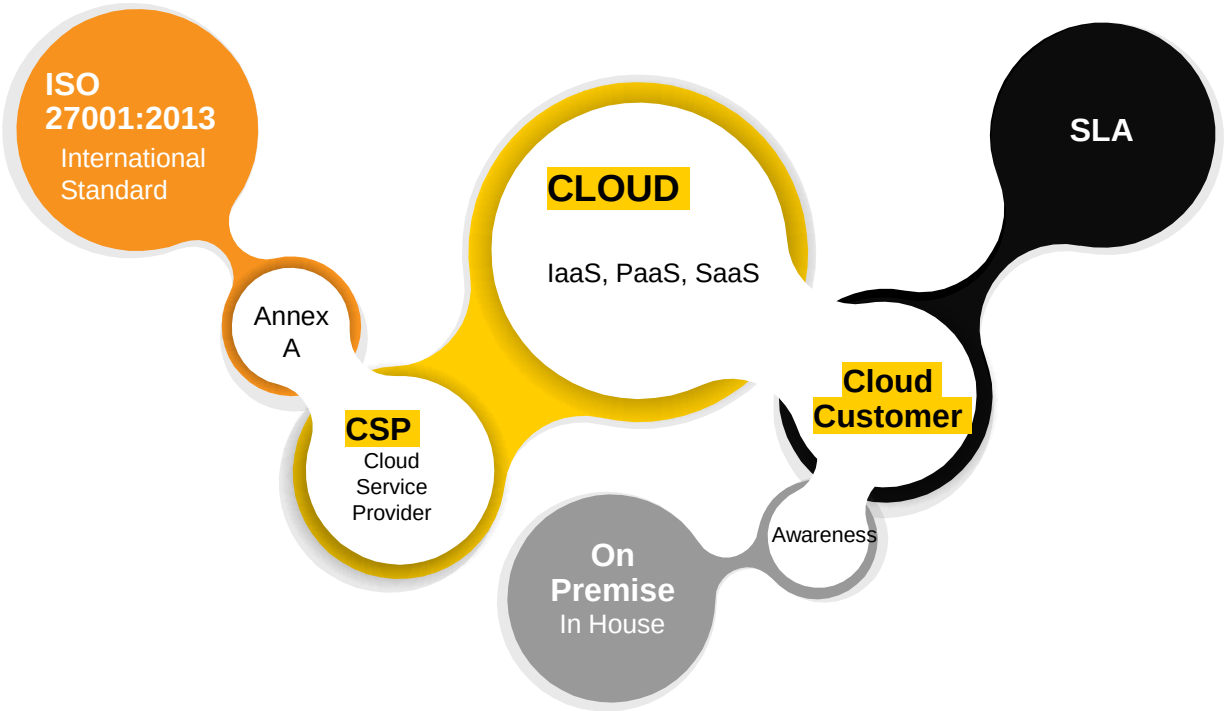
CRITERIA 3
Relevant to Cloud Computing?

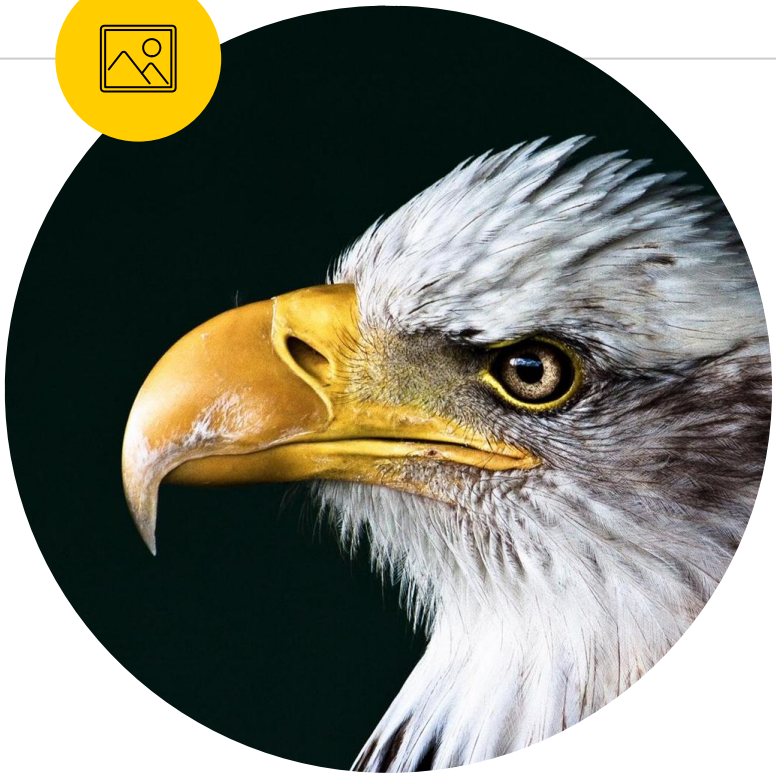
CRITERIA 4
Is it the base of a Cloud System?



(e.g. Incident Management and Business Continuity)

CONCEPT MAP


ISO 27001:2013
International Standard
Annex A
CSP
Cloud Service Provider
CLOUD
IaaS, PaaS, SaaS
SLA
Cloud Customer
Awareness
On Premise
In House



Tables for ISO 27001:2013's evaluation for Cloud Computing

TECHNICAL REPORT · JULY 2015

DOI: 10.13140/RG.2.1.4683.7603

READS

61

2 AUTHORS:

Muhammad Imran Tariq

Superior University

11 PUBLICATIONS **10** CITATIONS

SEE PROFILE

Vito Santarcangelo

Centro Studi , Buccino (SA), Italy

34 PUBLICATIONS **12** CITATIONS

SEE PROFILE

Muhammad Imran Tariq[1], Vito Santarcangelo[2]
1 Superior University, 36-L, Gulberg-III, Lahore, Pakistan
2Centro Studi S.r.l, Zona Industriale, Buccino

imrantariqbutt@yahoo.com, vito.santarcangelo@centrostudi.biz

Tables for ISO 27001:2013's evaluation for Cloud Computing

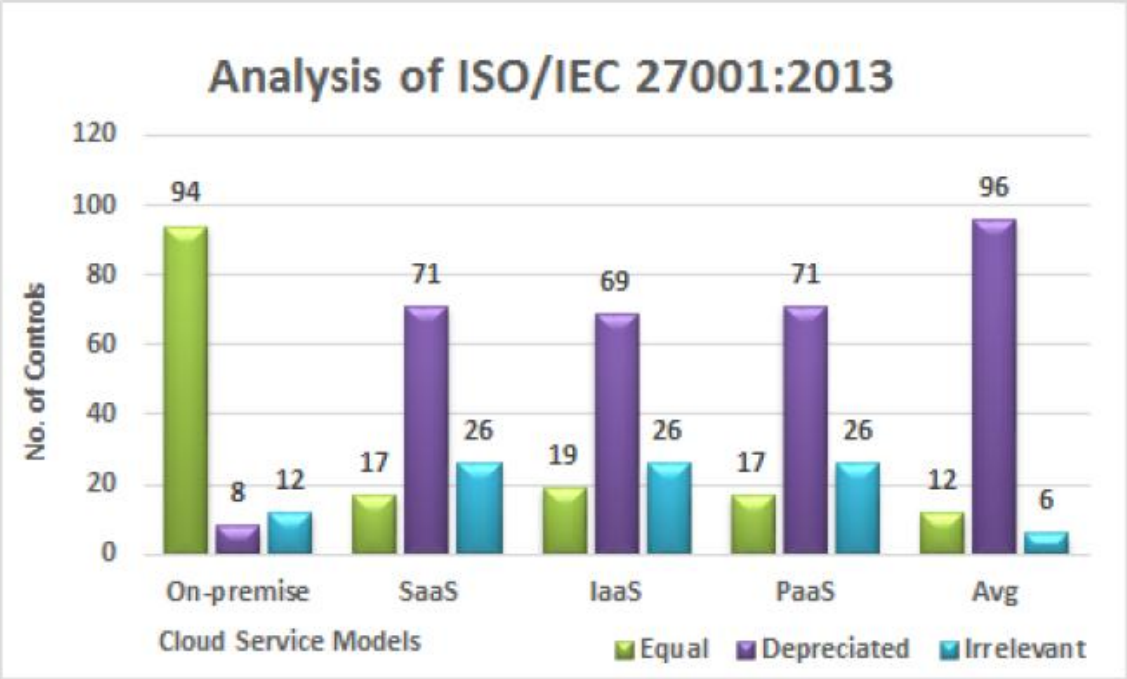
Table 3: Evaluation of ISO / IEC 27001: 2013

Control	Private	Public			Avg	SLA	Related	Fundamental	Total
	On-premise	SaaS	IaaS	PaaS					
A.5 Information security policies	5	0	0	0	1	1	1	0	3
A.5.1 Management direction for information security	5	0	0	0	1	1	1	0	3
A.5.1.1 Policies for information security	5	-	-	-	1	1	1	0	3
A.5.1.2 Review of the policies for information security	5	-	-	-	1	1	1	0	3
A.6 Organization of information security	5	1	2	2	2	1	1	1	4
A.6.1 Internal organization	4	0	0	0	1	0	1	0	3
A.6.1.1 Information security roles and responsibilities	5	-	-	-	1	1	1	0	3
A.6.1.2 Segregation of duties	5	-	-	-	1	1	1	0	3
A.6.1.3 Contact with authorities	3	-	-	-	1	0	1	0	2
A.6.1.4 Contact with special interest groups	4	-	-	-	1	0	1	0	2
A.6.1.5 Information security in project management	5	-	-	-	1	0	1	0	2
A.6.2 Mobile devices and teleworking	5	1	4	3	3	1	1	1	6
A.6.2.1 Mobile device policy	5	1	4	3	3	1	1	1	6

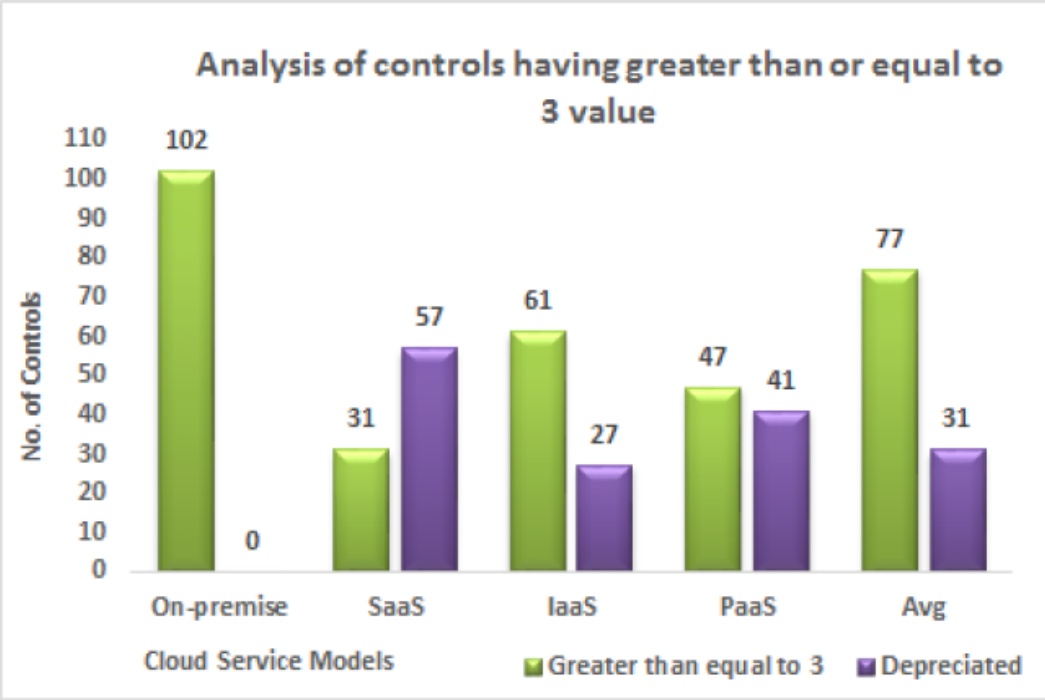
Control	Private	Public			Avg	SLA	Related	Fundamental	Total
	On-premise	SaaS	IaaS	PaaS					
A.9.4 System and application access control	5	1	3	2	3	1	1	1	6
A.9.4.1 Information access restriction	5	1	4	3	3	1	1	1	6
A.9.4.2 Secure log-on procedures	5	1	4	2	3	1	1	1	6
A.9.4.3 Password management system	5	1	1	1	2	1	1	1	5
A.9.4.4 Use of privileged utility programs	5	1	2	2	3	1	1	1	6
A.9.4.5 Access control to program source code	5	3	3	3	4	1	1	1	7
A.10 Cryptography	5	1	5	2	3	1	1	1	6
A.10.1 Cryptographic controls	5	1	5	2	3	1	1	1	6

Control	Private	Public			Avg	SLA	Related	Fundamental	Total
	On-premise	SaaS	IaaS	PaaS					
A.16 Information security incident management	5	2	3	2	3	1	1	1	6
A.16.1 Management of information security incidents and improvements	5	2	3	2	3	1	1	1	6
A.16.1.1 Responsibilities and procedures	5	5	5	5	5	1	1	1	8
A.16.1.2 Reporting information security events	5	1	3	2	3	1	1	1	6
A.16.1.3 Reporting information security weaknesses	5	1	3	2	3	1	1	1	6
A.16.1.4 Assessment of and decision on information security events	5	1	3	2	3	1	1	1	6
A.16.1.5 Response to information security incidents	5	1	3	2	3	1	1	1	6
A.16.1.6 Learning from information security incidents	5	1	1	1	2	1	0	1	4
A.16.1.7 Collection of evidence	5	2	3	3	3	1	1	1	6
A.17 Information security aspects of business continuity management	5	5	5	5	5	1	1	1	7
A.17.1 Information security continuity	5	5	5	5	5	0	1	0	7
A.17.1.1 Planning information security continuity	5	5	5	5	5	0	1	0	6
A.17.1.2 Implementing information security continuity	5	5	5	5	5	0	1	0	6
A.17.1.3 Verify, review and evaluate information security continuity	5	5	5	5	5	0	1	0	6
A.17.2 Redundancies	5	5	5	5	5	1	1	1	8
A.17.2.1 Availability of information processing facilities	5	5	5	5	5	1	1	1	8
A.18 Compliance	5	4	4	4	5	1	1	1	7
A.18.1 Compliance with legal and contractual requirements	5	5	5	5	5	1	1	0	7

ISO & CLOUD


Analysis of ISO/IEC 27001:2013
No. of Controls
120
100
80
60
40
20
0
94
8
12
17
71
26
19
69
26
17
71
26
12
96
6
On-premise
SaaS
IaaS
PaaS
Avg
Cloud Service Models
Equal
Depreciated
Irrelevant

ISO & CLOUD


Analysis of controls having greater than or equal to 3 value
No. of Controls
110
100
90
80
70
60
50
40
30
20
10
0
102
0
31
57
61
27
47
41
77
31
On-premise
SaaS
IaaS
PaaS
Avg
Cloud Service Models
Greater than equal to 3
Depreciated

CONSIDERATIONS

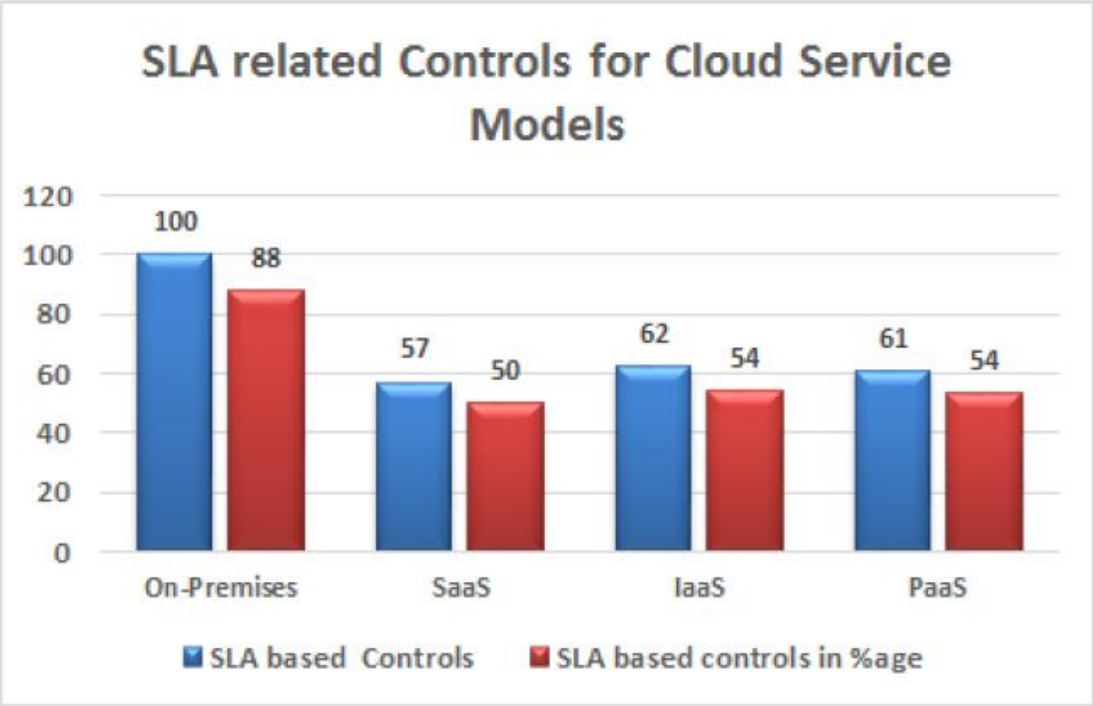
ISO 27001 Annex A is a very important flexible approach that **allows CSP to decide what level of risk is acceptable** (in line with business objectives) and the needed controls to reach the target.

The **ISO 27001 standard is generic standard** that covers all management, operational, technical areas to deal with threats and vulnerabilities. Due to its generic nature, **it does not cover all Cloud information security system challenges**.

To sum up, the analysis shows that ISO 27001:2013 **provides a good reference** to create a secure Cloud Computing, however it's necessary that the CSP is committed to Information Security. **Cloud Service Provider needs to include these aspects in risk assessment that are directly related to Cloud Computing**.

The research also find out the number of the controls which can be used during the development of SLA between both customer and CSP.

SLA & CLOUD



57 out of 114 controls can be used in Service Level Agreement which is based on Software as Service (SaaS). The Platform as Service has 61 controls and Infrastructure as Service has 62 controls that can be used in a Service Level Agreement.

Cloud customer is required to implement standard controls to maintain its information security, in-house assets, personal and deal with legal obligations, etc.

CONCLUSIONS

In conclusion, this research adopts ISO/IEC 27001:2013 as Information Security Standard while the **other Information Security Standards** like COBIT, GAISP, SSE-CMM, FISMA, ISNI/ISA 99 and NIST **can also be used to map the security risks** and to increase the volume of this study.

Moreover, real time and practical issues will be improved through interview, questioners and other techniques with Cloud stakeholders.

As future work, the **other security standards** will be **evaluated** and quantified in addition to the existing Cloud risk database to provide their importance and effectiveness more accurately to the Cloud customer.

Thanks!

Any questions ?

You can find me at

- vito.santarcangelo@centrostudi.biz

http://www.researchgate.net/profile/Vito_Santarcangelo

Credits

Special thanks to all the people who made and released these awesome resources for free:

- Presentation template by SlidesCarnival
- Photographs by Unsplash