Increasing Security Guidelines' Framework Efficiency

Yury Chemerkin
Russian State University for the Humanities (RSUH), Moscow, Russia

Abstract

There are many security guidelines, standards and best practices are well-known for almost all occasions on information security field but the cloud case is still young. We have different security requirements and metrics based on new frameworks that revolutionize and simplify a usual security model in a cloud manner. However, the transparency of 'paper' requirements and real cloud features is beyond the scope of these guidelines and is a matter of discussion.

Keywords: cloud security, cloud computing, amazon web services, aws, azure, compliance, csa recommendations, bes,, nist sp 800-53 rev.4, nist, csa, iso 27001, iso 27001'13, iso

1. Introduction

Nowadays, a cloud security is a new "security through obscurity" spiral of security and frameworks based on it. For example, a public cloud hypervisors (sometime private cloud hypervisors are too) do not provide controls to manage any processes or flows that is a target of a blackbox pentest and risk management methods. This raises more transparency questions instead of reducing it. In previous work [5] were shown conceptual means related to incorrect conclusions formed in the mind like vulnerability attacks applicability to any clouds are it private clouds or public clouds. A weak granularity is another problem of young guidelines, for example, not all requirements are clear in according to the roles and responsibilities of cloud vendors and their customers because it makes uncertain whether the vendors should provide the customers any control opportunities and could leads to swapping responsibilities and shifting vendor job on to customer shoulders [1].

To build a security and privacy, cloud vendors provide their customers with security controls on areas like data protection, identity management, application and system/network security, availability, patch management, application and email management, etc. Additionally, cloud computing has become a universal background for many software services and solutions even mobile device management solutions. Thus, cloud guideline frameworks are still young decrease its efficiency and transparency by necessity to solve various problems and provide certain security level.

This research examines cloud guidelines frameworks and security model in alignment public cloud like Amazon Web Services, Microsoft Azure. It addresses to devising methods of managing requirements' cases in according cloud model differences. In other words, this research proposes a sub-framework that extend existing NIST framework and significantly improve existing security models from NIST SP 800-53, ISO 27001'2013, and CSA guidelines. This paper extends the results of previous [5-6] on security, compliance and transparency of public clouds.

2. Related work

2.1. Cloud Model Results

Clouds are growing day by day with different cloud-based services and large number of vendors. There are several common types of cloud service models: IaaS, PaaS, SaaS; each of them has its own distinctive features.

- **IaaS** – physical or virtual machines and other resources, such as VLANs, IP addresses, firewalls, block, blob and file-based storages, load balancers, etc. AWS is one IaaS cloud models that offers DynamoDB, Elastic Block Store, Elastic Compute Cloud, Route 53, Simple Email Service and other services.
- **PaaS** –a kind of development environment that offers its customers access to components for executing their respective applications. It is typically including operating system, execution environment, database, and web server like Microsoft Azure.
- **SaaS** – it provides access to any user to use software and databases on-demand without installing it, such as CMS or mobile MDM

IaaS is designed for maintaining control of software environment and virtual equipment and not caring about physical equipment. This model grows itself quickly, but not market at all. SaaS is geared toward the end users and does not take much to get started. This model grows quicker than other does. PaaS is somewhere in between IaaS and SaaS; a kind of non-finished product, such as IDE as a set of tools to develop mobile apps, social apps, websites, games, databases, etc.[17].

Cloud model specifics based on features were implemented into certain model type and reflects a control granularity:

- **IaaS** – the cloud users have the maximum control over this cloud model. It usually includes prebuild web-console (or another type of console) to manage a cloud, NaaS (network) management system, permissions and APIs to run out 100% coverage.
- **PaaS** – the cloud users have the medium control over this cloud model. It includes the basic controls to manage cloud and have a difference between cloud storage like Dropbox and Amazon S3 service, where the first has three permissions (owner access, custom set access, public access) and the second has separate permission vs. one API method.
- **SaaS** – the cloud users have the least control over this cloud model. Controls usually depend on software type; in case of MDM, it gives mobile email and application management features; in case of CMS, it gives author management features to separate access to data, wallet and moderation.

2.2. CSA Compliance Results

CSA guidelines pretends to a superstructure over other documents, such as NIST, ISO, and PCI DSS. In other words, CSA documents are written as a generalized abstraction: it has basic framework and set of requirements are mapped to similar requirements of another guideline. CSA documents still not enough detailed and do not go deeply enough on control than other, e.g. NIST has several control layers – basic, enhanced and dependence layers. Also, CSA guidelines refer to the cloud treats and issues that outdated:

1) **OpenSource (OpenStack)**

Most cloud providers expose APIs that are typically well documented and adopted others' APIs a view to delivering interoperability and portability. This project is OpenStack and as of end of that year OpenStack supporters include AMD, Intel, Canonical, SUSE Linux, Red Hat, Cisco, Dell, HP, IBM, Yahoo and now VMware. According to CSA, top public clouds like Azure or AWS are not among these supports. In fact, OpenStack is compatible with Amazon EC2 and Amazon S3 and thus client applications written for AWS can be used with OpenStack with minimal porting effort. Moreover, in this case, SaaS cloud models are not mentioned in CSA documents even.

2) **Lock-In's**

In the course of OpenSource issues, Lock-In is a more detailed set of issues include:

Platform lock-in	Lack of Import/Export platform tools for migration from one cloud vendor to another.
Data Lock-in	Lack of tools for data migration.
Tools Lock-in	Lack of universal tools to manage any cloud.
APIs Lock-In	Lack of OpenStack APIs (see OpenSource paragraph)

CSA statement on platform lock-in: CSA statement: private clouds high-probability have these tools than public; in fact, AWS have tools to migrate from/to VMware, while Azure does not have. CSA statement on data lock-in: private clouds high-probability have these tools than public; in fact, AWS has native solutions linked with Cisco routers to upload, download and tunneling as well as 3rd party storage like SMEStorage (AWS, Azure, Dropbox, Google, etc.)

Lack of transparency has grown up on matter that cloud vendors address to NDA reports written by third party auditors and experts as a part of SAS 70 compliance in most cases. It disrupts a bond of 'roles and responsibilities' and what controls are configurable and available to customers. The rest is about lack of technical transparency: CSA guidelines focuses on organization-defined control than technical.

According to previous papers, the results in regards to CSA guidelines could be figured out:

- basic framework is not worked out for cloud models
  - IaaS may have more controls than CSA documents have;
  - PaaS controls usually defined by development best practices;
  - SaaS has sector-driven controls.
- superstructure over other guidelines and standards
- pure detailed elaboration in regards to requirements
- outdated with strong dependence to its parts
- lack of transparency due to a pure map-matrix and SAS-70 compliance

CSA publication has a pure 'roles & responsibility matrix' that corroborates the various interpretations of this recommendations given in guidelines. It has only one 'Consumer Relationship' recommendation - SA-13 "Location-aware technologies may be used to validate connection authentication integrity based on known equipment location". In turn, 'Vendor Relationship' recommendations include other and all technical and management solutions, while 'Consumer Relationship shared with Vendor' controls include non-technical solutions only, such as, policies, roles, procedures, training.

3) **AWS & Azure Examination**

Paper contains examinations in regards to IaaS cloud model (AWS), PaaS cloud model (Azure) in alignment CSA and NIST requirement under basic and enhanced controls (control layers). Results highlight a pure difference between CSA control layer as well as cloud models and significant one on NIST guidelines. NIST provides technical details to cloud controls and point out to a distinction between IaaS and PaaS cloud models.

3. GUIDELINES FRAMEWORK

2.3. CSA Framework

Goal of CSA guidelines is restructuring information about cloud controls to help customers easy meet with requirements, quickly find a connection with another standards. It contains 100+ cloud-related controls divided into two parts (basic and enhanced security requirements), cloud model structure and compliance model matrix. Cloud model structure describes by following components are part of IaaS, PaaS, and SaaS [2-4]:

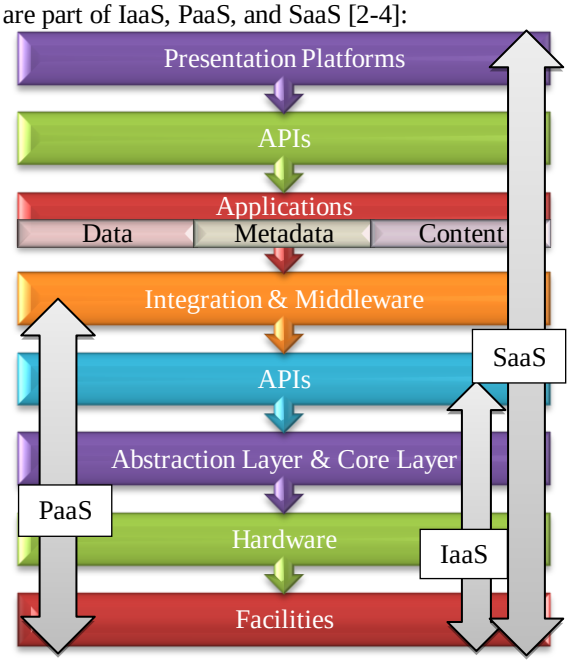

Figure 1. CSA cloud model types

Compliance model matrix allows remapping CSA requirements to requirements of following industry-standards:

- COBIT 5
- HIPAA/HITECH act
- ISO/IEC 27001-2005
- FedRAMP
- PCI DSS v2.0
- BITS Shared Assessments AUP v5.0/SIG v6.0
- GAPP
- NIST 800-53 rev.3

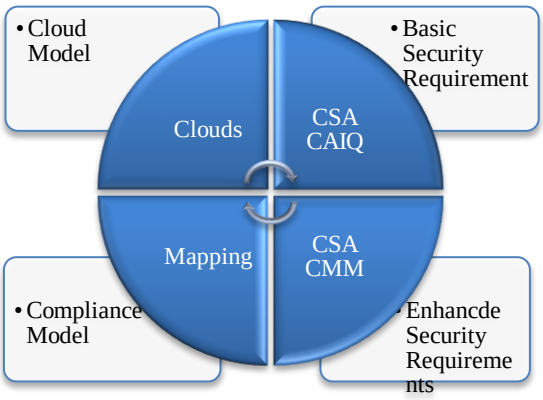

Figure 2. CSA Framework

Typical Control Structure is presented on *Figure 3*

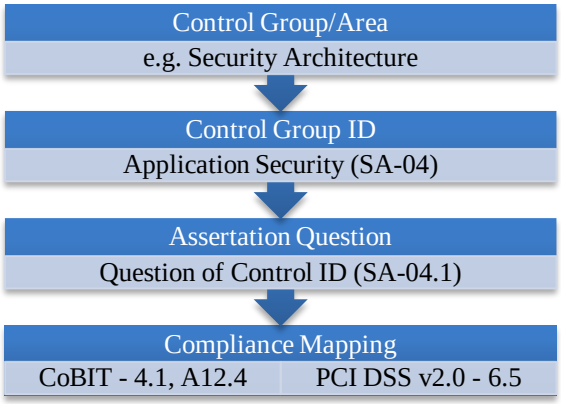

Figure 3. CSA Control structure

2.4. NIST Framework

NIST provides guidelines for selecting and specifying security controls for organizations and information systems and apply to all components of an information system that process, store, or transmit information. NIST series [13-16] based on the same framework and methodology; each document describe in details certain part, so that SP 800-53 is totally focused on technical controls while SP 800-39 provides guidance on risk management describing three tiers of risk:

- organization level (Tier 1) - management with respect to information security'
- mission/business process level (Tier 2),
- and information system level (Tier 3) – is to select security controls.

The last Tier (3) refers to SP 800-53 publication [15] and contains all security controls. Additionally, this Tier defines so-called Risk Management Framework (RMF) composed of six steps, two of them (*steps two, six*) refer to that publication too

- Step 2. A selection an initial set of baseline security controls for the information system based on system impact level and apply tailoring guidance, as needed;

- Step 6. Monitoring the security controls in the information system and environment of operation on an ongoing basis to determine control effectiveness, changes to the system/environment, and compliance to legislation, policies, regulations, and standards.

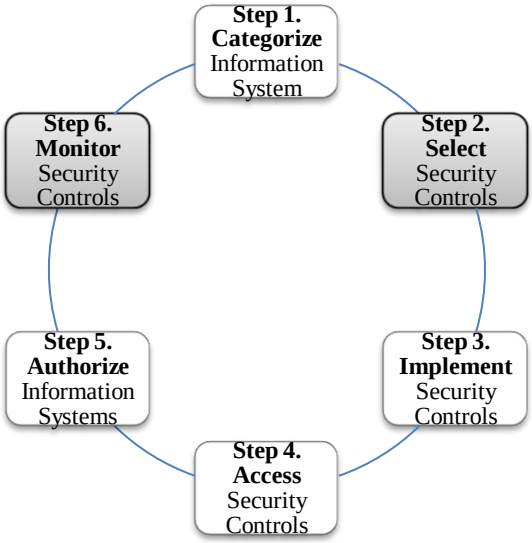

Figure 4. NIST Framework (RMF)

NIST SP 800-53 rev3 "Recommended Security Controls for Federal Information Systems and Organizations" include following controls:

- common controls;
- external environments;
- security control assurance;
- tailoring and supplementing the baseline

These security controls are organized into eighteen families (SP 800-53 rev4). Each family contains security controls related to the general security topic of the family marked a two-character identifier, such as Personnel Security – PS.

Table I. Security control ID and family names

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

The last family (PM, Program Management) is beyond of that publication (SP 800-53) while the similar section of CSA publication is significant. Part of this section [PM] is the master control requiring an insider threat program, including a team that is focused on insider threat incident handling. The program should include security controls that require such monitoring and correlation. This section is up to organization entirety.

Each security control has its structure described below. The ***control section*** describes specific security-related activities or actions that generally involve the implementation of hardware, software, firmware, etc. The ***supplemental guidance section*** provides additional information related to a specific security control from previous section, but contains no additional requirements. It means it is possible to apply the supplemental guidance as appropriate, when defining, developing, and/or implementing security controls. Also, this section may contain a list of related controls that:

- directly impact or support the implementation of a particular security control or control enhancement;
- address a closely related security capability; or
- are referenced in the supplemental guidance.

The ***security control enhancements section*** provides statements of security capability to add functionality/specificity to a control; and/or increase the strength of a control. This section may also contain supplemental guidance, typically provided in situations where the guidance is not generally applicable to the entire control but instead focused on the particular control enhancement. The ***references section*** includes a list of applicable federal laws, policies, regulations, standards, and guidelines. The ***priority and baseline allocation section*** provides the recommended priority codes used for sequencing decisions during security control implementation; and the initial allocation of security controls and control enhancements to the baselines for low-impact, moderate-impact, and high-impact information systems.

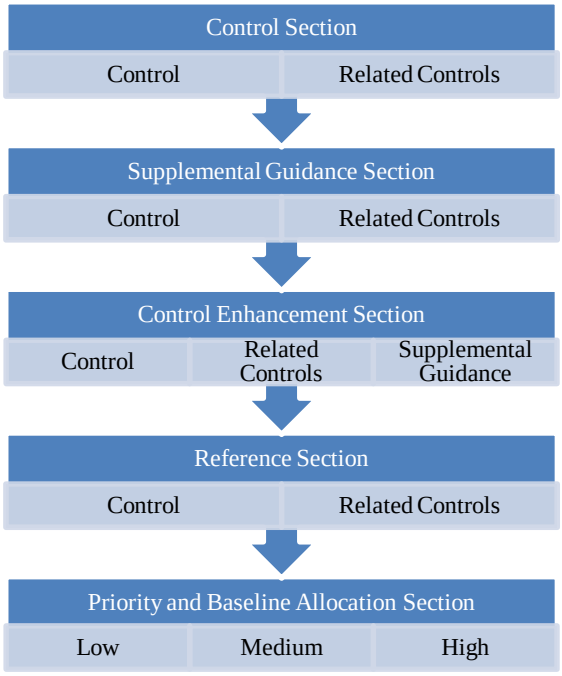

Figure 5. NIST control structure

4. NIST SP 800-53 REV4 EXAMINATION

This research proposes a sub-framework as a way to extend existing NIST framework and significantly improve existing security models from NIST, ISO, and CSA guidelines. Additionally, this sub-framework is going to be adopted on different cloud models IaaS, PaaS, SaaS in regards AWS, Azure, BlackBerry Enterprise Server (BES) as a Mobile Device Management service (MDM). To achieve it, the following examination must be done:

- revise changes of NIST rev3 and rev4;
- revise changes of ISO-27001'2005 and 2013 edition;
- make an analysis of guidelines model limits as it was done in case of CSA publication;
- remap requirements between guidelines are recently released;
- work out sub-framework to improve existing CSA;
- adopt on different cloud models.

2.5. NIST SP 800-53 rev4

First, of all we need analysis what exactly changed in new revision of NIST publication [16]. The fourth revision has new requirements and countermeasures including on mobile and cloud issues. That part of requirement refers to another publication, such NIST SP 144-146, that describes different cloud environments (models), SLA and API issues and a set of so-called open issues are not addressed by cloud providers, e.g. information security and compliance. Several qualities amendments and modifications are in new revision:

Baselines Part include many new controls and control enhancements have been added, some of them moved to optional in alignment internal and external environments, new threats like APT, mobile, cloud and additional **privacy section** control added; it finally are around 450 controls. Separated **Families** are mentioned above were regrouped into three big classes: management, operational, technical. Several new controls are on *Table II. New ISO controls*

Table II. New ISO controls

Family	Controls
PM Family	12, 13, 14, 15, 16
AC Family	23, 24, 25
AU Family	15, 16
CA Family	8, 9
CM Family	10, 11
CP Family	11, 12, 13
IA Family	9, 10, 11
IR Family	9, 10
MP Family	7, 8
PE Family	20
PL Family	7, 8, 9
RA Family	6
SA Family	15, 16, 17, 18, 19, 20, 21, 22
SC Family	35, 36, 37, 38, 39, 40, 41, 42, 43, 44
SI Family	14, 15, 16, 17

New revision expands a term *Trustworthiness* and its component *Assurance*; new *Functionality* component was added and determined by the security features and functions employed within information systems and their operating environment.

Overlays, is a new part in regards cloud computing, mobile devices, new environments, threats and specific regulatory requirements, allow a commonly used set of tailoring changes to be applied across many areas. This section was designed to increase assurance when connections between systems are desired. Overlays can be developed for a wide variety of viewpoints:

Privacy is one more part that is new brings privacy controls and control enhancements on following areas:

- Authority and Purpose (AP);
- Accountability, Audit, and Risk Management (AR);
- Data Quality and Integrity (DI);
- Data Minimization and Retention (DM);
- Individual Participation and Redress (IP);
- Security (SE);
- Transparency (TR);
- Use Limitation (UL).

The final change is a mapping of controls to Common Criteria (ISO 15408). NIST rev4 has a map references to old ISO edition (2005).

Key problems include a lack of cases and examples which component and requirements should be implement on cloud or mobile issues, some of them are missed, such as Session Lock that was defined for classic environments only but available for mobile and cloud environments too. Also, remapping from one guidelines to another does not include related controls (it could be), all enhance-based control, such as tailored, enhanced,

etc. (it couldn't be, NIST only controls). Remapped controls from NIST rev4 to ISO'2013 is available on [18], NIST rev4 → ISO'2005 connection is available on [18], CSA→NIST rev3 is available in CSA publication [16] but contains couldn't be used due to lack of cloud controls has come in next (fourth) revision of NIST, NIST rev4 → CSA connection is beyond this paper due to many assumptions should perform and a matter of further research.

2.6. ISO 27001'2013

ISO rev.2005 was not enough technical-oriented guidelines and the major change of new revision is being closer to enterprise risk management more that reflected in almost each clauses (requirements/controls in terms of ISO). One more change that is similar is changing context to an organization rather than a physical or a logical boundary. Like NIST rev4, ISO has added clauses that are either new or are more specific in the new standard:

Table III. ISO'13 changes

Control ID	Description of control	Changes
A.6.1.4	Information security in project management	this is a new clause on PM
A.6.2.1	Mobile device policy	more specific in new edition
A.8.3.3	Physical media transfer	more specific in new edition
A.9.2.1	User registration and de-registration	more specific in new edition
A.9.2.3	Management of secret authentication information of users	this focuses on handling sensitive authentication data such as a password
A.9.2.5	Removal or adjustment of access rights	considers 'adjustment' of access
A.9.4.4	Use of privileged utility programs	renaming 'use of system utilities'
A.13.2.1	Information transfer policies and procedures	renaming 'policy on exchange of information'
A.14.1.1	Security requirements analysis and specification	more elaborate clause in new edition
A.14.1.2	Securing applications services on public networks	more specific in new edition
A.14.1.3	Protecting application services transactions	more specific in new edition
A.14.2.6	Secure development environment	this is a new clause
A.14.2.8	System security testing	this is a new clause
A.15	Supplier relationships	this is a new domain
A.15.1.1	Information security policy for supplier relationships	this is a new clause
A.15.1.2	Addressing security within supplier agreements	this is a new clause

Key problems are major changes were made in alignment with business strategy, secure development life cycle and a focused incident response process than security controls. Remapped controls from ISO'2005 to ISO'2013 is available on [18], ISO'2013 to NIST rev4 is available on [18], CSA → ISO'2013 could remapped throughout ISO'2005 → ISO'2013 table due to narrow difference as both publication (CSA, ISO) were written in alignment business strategy and risk management context.

2.7. Cloud Sub-Framework and adoption on different cloud models

Let us summarize pros and cons of mentioned publications in following table:

Table IV. Pros and cons vs. cloud guidelines

	Statement	Pros	Cons
CSA	Unifying recommendations for all clouds	Being superstructure	Adoption by publications filled out by cloud vendors;
CSA	Unifying recommendations for all clouds	All requirements cover SaaS, PaaS, IaaS cloud types	Fail on cloud model difference
CSA	Relationship to other industry standards: PCI DSS, ISO, COBIT, NIST, FEDRAMP	Work out for risk management guidelines	Many assumption on technical part (e.g. NIST connection)
CSA	Cloud Model	Elaboration on all layers	Lack of clearly defined responsibilities
CSA	Recommendation style	Attempt to let professionals share their vision on cloud security in alignment this publication	A lot of references on 3rd party reviewers under NDA (SOC 1 or SAS 70) + outdated documents
CSA	Recommendation style	New structure more related to manage resources	Different explanation by each vendor of the same recommendation
ISO	Framework	New revision include specifics clauses (controls)	Shifted to risk management and not written as a 'specific' (like a cloud or mobile) publication

CSA	Framework	Risk management context	SDLC interpretation that is good for PaaS cloud model up-to-now
NIST	Framework	Universal among series publications	-
CSA	Relationship to other industry standards: ISO, Common Criteria, FIPS	Work out in both directions	Own series of publications, a weak relationship to other series
NIST	Framework	Several layer of security and enhancements	Self-defining a set of controls are applicable for certain environments by technical features of it
NIST	Complementarity	Replacing basic controls by enhanced controls and possibility to define customer own specifics control and relationship	-
NIST	Framework	Provide different publications on audit logging, activity reporting, security controlling and data retention	Publications refer to that [800-53 rev4] publication is not enough elaborated and missed details
NIST	Recommendation style	Classic style, good for full-detail and well-documented solutions; applicable for specific local regulation and standards, like Russian publications	Classic style, complex from resource-based viewpoint

Examination of cloud guidelines in regards of high growth cloud computing industry and different cloud models leads to need of modelling methods of managing requirements' (controls) in a state of uncertainty and differences of cloud technical specifics. NIST framework provides interchangeability and expansibility to its publications that means the framework is open to redefine part and supplement new controls in new cases. It is strengths, because there are many models and architectures and many ways to build cloud in alignment to certain requirements and technical capabilities of operated solutions and environments.

Proposed sub-framework represent on *Figure 6*; it redefines the first step of RMF and extend the second of RMF. The concept of the first step is choosing a predefined guideline in regards to cloud computing model type. It is based on results of examination [7-9]; in case of SaaS, combination of several guidelines is better but depends on sector type, e.g. MDM may require more enhanced controls than CMS. Main concept of the second step divides intro three groups:

- first group is based on scope of applicability controls to environment – it depends on activities or way how to manage controls;
- second group is based on a selection of family class – it is a kind of predefined granularity of control;
- third group is based on a granularity controls – it depends on different aspects may include risk/treat model and countermeasures; for example, turn on/off state has a low granularity and do not require complex solution, while building API-based restricted solution, including heuristic detection does require highly detailed custom set of controls

The first group includes two scopes - Resource-based and Feature-based scope of managing controls, where CSA guidelines is better to apply to the resource-based scope, NIST to another scope; in case of necessity, it should be combined together. The second group includes three control families, each of them is better predefined to certain guidelines (Operational is for ISO, Management is for CSA, Technical is for NIST). The third group define granularity as four levels (custom, high, medium, low) reassigned to following cases:

- Combine several guidelines' requirements together;
- Apply enhanced control from NIST;
- Apply enhanced control from CSA, or basic controls from NIST; in case of need, it is possible to remap CSA to NIST to quickly define an appropriate set of controls;
- Apply basic controls from CSA, ISO;

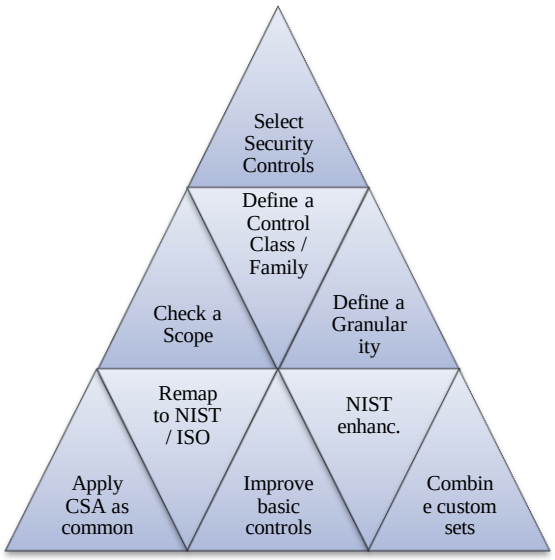

Figure 6. Cloud subframework

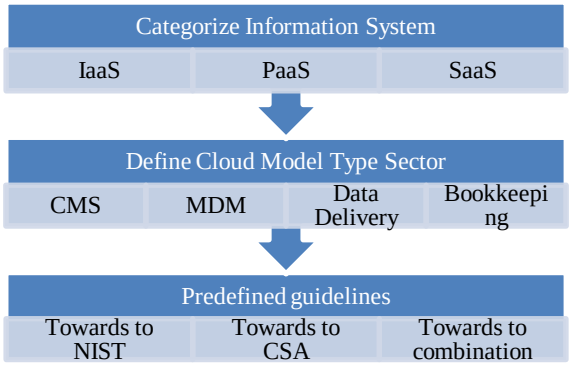

Figure 7. Extension of the RMF's Step 1

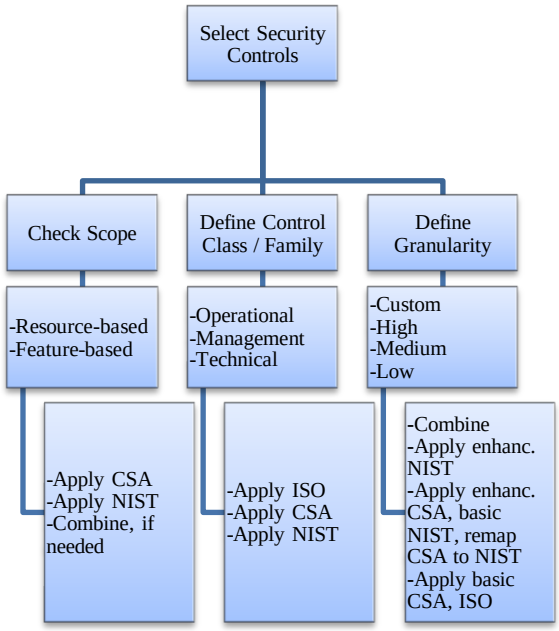

Figure 8. Extension of the RMF's Step 2

To make it clear, let us give an example per each cloud model (SaaS was examined in [7-8] it is discussed briefly below).

Azure [10] is a PaaS model has belonged to distribution of information sector (*step #1 extension is done*). Family control class is management, in term of CSA it is *Data Governance*, in term of NIST it is a set of *access control*, *media management*, etc. (actually, it must be remapped from CSA to NIST). Data Government includes the following controls each of them corresponds to NIST control one with certain assumptions:

Table V. Remapping CSA controls to NIST controls

CSA	**NIST**
Ownership / Stewardship	Access control
Classification	Should be done before selecting controls
Handling / Labeling / Security Policy	Access Control / Security Attributes
Secure Disposal	Has similar group of controls
Non-Production Data	- (CSA or ISO only), possible to remap from NIST to ISO
Information Leakage	Access control + Media management (assumption)
Risk Assessments	PM section, is beyond of 800-53 publication

In this case, it is easy to use CSA than pick up NIST controls from different group, however, NIST is applicable as a custom controls' collection, if it needed.

AWS is an IaaS model has belonged to various type of sector and primary not a data distribution. AWS has many technical controls to manage users, resources, or complex security configurations through a custom controls' collection. Thus, it is towards the NIST publication that has an '*Access Control*' control groups including:

- Account, Session Management;
- Access / Information Flow Enforcement;
- Least Privilege, Security Attributes;
- Remote / Wireless Access.

In this case, NIST has special enhancements in the fourth revision, for example, '*Account Monitoring - Atypical Usage*' that directly corresponds and applies to AWS S3 log gathering native feature. Other controls could be directly applied too:

- Dynamic Account Creation;
- Restrictions on Use of Shared Groups – Accounts;
- Group Account Requests Approvals/Renewals;
- Account Monitoring - Atypical Usage.

AWS [11] has many services and could be turn into PaaS model or be used for data spreading which case is good for combining NIST and CSA together. *Data Governance* (CSA) controls is applicable from the resource-based viewpoint,

because AWS has a *Resource based policy*. In other words, such policy attaches to resources (*Figure 9*, bucket policy.) On other side, *Access Control* (NIST controls) is applicable from the user-based viewpoint, because AWS has an *Account based policy*. In other words, such policy attaches to users, user groups, or different user custom sets (*Figure 9*, IAM Policy). Both policies are identical but depends on preferable way how to manage stuffs and what is should be manageable (resources or accounts).

BES [12] is a MDM services (cloud or/and desktop software installed on cloud virtual OS) directly manages MS Exchange to deliver emails, to access to users. BES user groups is based on a set of users are added to BES databases. All subsequent activities performs to BES user accounts only. Also, it is possible to reassign AWS accounts to MS Exchange accounts, and reassign MS Exchange account to BES accounts in turn. Finally, in this case, NIST is better to define one policy for MDM users to access internal network resources and combine it with a mobile policy (that policy defines permissions could requested by applications and black and white lists of applications) [9].

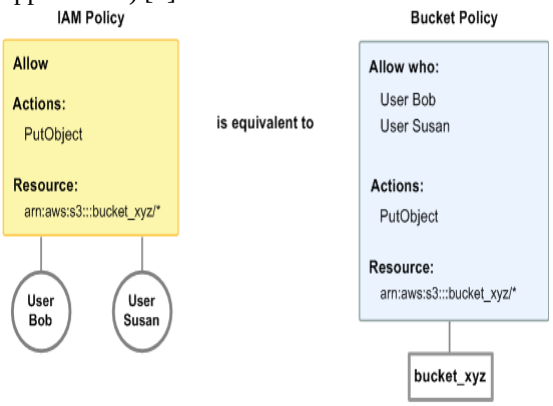

Figure 9. AWS Account-based and Resource-based Policy

5. Conclusion

With its increased adoption, various sectors cloud computing, security controls needs to be monitored and analysed frequently. From this paper, it is clear, there is a lack of '*cloud-feature-sensitive*' approaches in regards to cloud computing. Such approach could help reduce misunderstanding controls families, increase efficiency of managing complex cases, with different comprehensive approaches to management (operational, administrative, technical, etc.). Also, cloud customers can perform the control implementation in a security sensitive cloud by each cloud computing model type, where any discrepancy must shift the security level from the highest to one level lower and vice versa. It was discussed mainly three major models associated with cloud computing in terms of AWS, Azure, and BES clouds. With the rapid growth in that field, security mechanisms provided by the different cloud service providers must be eliminated to adopt framework up to another cloud features and certain cases that has significant importance of the framework. Finally, it helps to pick up appropriate set of controls due to the difference of these requirements and cloud capabilities and enhance a transparency of cloud controls.

6. References

[1] "CSA The Notorious Nine Cloud Computing Top Threats in 2013" [Online resource: downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf, Accessed 06-March-2013] .

[2] CSA Cloud Controls Matrix v1.3" [Online resource: cloudsecurityalliance.org/research/cai/, Accessed 15-January-2013].

[3] "CSA Consensus Assessments Initiative Questionnaire v1.1" [Online resource: cloudsecurityalliance.org/ research/cai/, Accessed 15- Jan-2013].

[4] "CSA Consensus Assessments Initiative Questionnaire v1.1" / CSA Cloud Controls Matrix v1.3" [Online resource: https cloudsecurityalliance.org/wp-content/uploads/2012/03/Microsoft-Azure-CAIQ-v1.1-2012-03-25.zip, Accessed 15-January-2013].

[5] Y. Chemerkin, "Limitations of Security Standards Against Public Clouds", Proceedings of the International Conference on Information Society (i-Society 2013), July, 2013.

[6] Y. Chemerkin, "Security compliance challenges on clouds", Proceedings of the Fifth International Conference on Internet Technologies and Applications (ITA 13), September 2013.

[7] Y. Chemerkin, Mobile Security from the BYOD's Viewpoint, CTICon-2013(II) - International Conference on "Exploring Global Transformations in Technology & Management", October 2013.

[8] Y. Chemerkin, Mobile Security Challenges on Compliance, CTICon-2013(II) - International Conference on "Exploring Global Transformations in Technology & Management", October 2013.

[9] Y. Chemerkin, Compliance and Transparency of Cloud Features against Security Standards, DeepSec Intel, September 2013.

[10] Windows Azure Security Overview whitepaper, [Online resource: go.microsoft.com/?linkid=9740388, Accessed: 01-Februarry-2013].

[11] BlackBerry Administration Documentation, [Online resource: http://docs.blackberry.com/en/ admin/?userType=2, Accessed: 15-December-2013].

[12] Amazon Security Center, [Online resource: https://aws.amazon.com/security/, Accessed: 15-December-2013].

[13] "Guidelines on Security and Privacy in Public Cloud Computing", [Online resource: csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf, Accessed 04-February-2013].

[14] "Cloud Computing Synopsis and Recommendations", [Online resource: www.nist.gov/ customcf/get_pdf.cfm?pub_id=911075, Accessed 04-February -2013].

[15] "Recommended Security Controls for Federal Information Systems and Organizations SP 800-53, revision 3", [Online resource: csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf, Accessed 04-February-2013].

[16] Security and Privacy Controls for Federal Information Systems and Organizations SP 800-53, revision 4, [Online resource: http://nvlpubs. nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf, Accessed 20-December-2013].

[17] IaaS vs. PaaS vs. SaaS, [Online resource: http://www.networkworld.com/news/2011/102511-tech-argument-iaas-paas-saas-252357.html, Accessed 20-December-2013].

[18] Additional materials on remapping controls [Online resource: https://sto-strategy.squarespace.com/ compliance/2014/1/6/remapping-security-controls-nist-sp-800-53-rev4-iso-270012013].

