In Proceedings of 2011 IEEE International Conference on Cloud Computing (CLOUD 2011), Washington DC, USA on 4 July – 9 July, 2011, IEEE

Collaboration-Based Cloud Computing Security Management Framework

Mohemed Almorsy, John Grundy and Amani S. Ibrahim
Computer Science & Software Engineering, Faculty of Information & Communication Technologies
Swinburne University of Technology, Hawthorn, Victoria, Australia
{malmorsy, jgrundy, aibrahim}@swin.edu.au

Abstract — **Although the cloud computing model is considered to be a very promising internet-based computing platform, it results in a loss of security control over the cloud-hosted assets. This is due to the outsourcing of enterprise IT assets hosted on third-party cloud computing platforms. Moreover, the lack of security constraints in the Service Level Agreements between the cloud providers and consumers results in a loss of trust as well. Obtaining a security certificate such as ISO 27000 or NIST-FISMA would help cloud providers improve consumers trust in their cloud platforms' security. However, such standards are still far from covering the full complexity of the cloud computing model. We introduce a new cloud security management framework based on aligning the FISMA standard to fit with the cloud computing model, enabling cloud providers and consumers to be security certified. Our framework is based on improving collaboration between cloud providers, service providers and service consumers in managing the security of the cloud platform and the hosted services. It is built on top of a number of security standards that assist in automating the security management process. We have developed a proof of concept of our framework using .NET and deployed it on a testbed cloud platform. We evaluated the framework by managing the security of a multi-tenant SaaS application exemplar.**

Keywords: cloud computing; cloud computing security; cloud computing security management

I. INTRODUCTION

The cloud computing model represents a new paradigm shift in internet-based services that delivers highly scalable distributed computing platforms in which computational resources are offered 'as a service'. Although the cloud model is designed to reap uncountable benefits for all cloud stakeholders including cloud providers (CPs), cloud consumers (CCs), and service providers (SPs), the model still has a number of open issues that impact its credibility.

Security is considered one of the top ranked open issues in adopting the cloud computing model, as reported by IDC [1]. A reasonable justification of such increasing concerns of the CCs about cloud security [2] includes: (1) The loss of control over cloud hosted assets (CCs become not able to maintain their Security Management Process (SMP) on the cloud hosted IT assets); (2) The lack of security guarantees in the SLAs between the CPs and CCs; and (3) the sharing of resources with competitors or malicious users. Accordingly, no matter how strongly the model is secured, consumers continue suffering from the loss of control and lack of trust problems. On the other hand, the CPs struggle with the cloud platform security issues because the cloud model is very complex and has a lot of dimensions that must be considered when developing a holistic security model [2] including the complex architecture of the cloud model, the model characteristics, the long dependency stack, and the different stakeholders' security needs. These dimensions result in a large number of heterogeneous security controls that must be consistently managed. Moreover, the CPs host services they are not always aware of the contents or the security requirements to be enforced on these services. This leads to a loss of security control over these services and the cloud platforms.

Although much research into cloud services security engineering has been undertaken, most efforts focus only on the cloud based services offered, such as web services. Such efforts have investigated capturing security requirements and generating corresponding WS-Security configurations. However, they pay no attention to the underlying platform security or the other cloud service delivery models such as IaaS and SaaS. They also do not address the impact of the multi-tenancy feature introduced by the cloud model on the security of the cloud delivered services.

Two new community projects are trying to tackle the CCs trust problem by introducing a list of best practices and checklists such as CSA - GRC project [3], or by aligning existing security standards to the cloud model such as FedRAMP [4]. Both projects' focus is to obtain CCs trust by assessing and authorizing the cloud platforms. These projects lack the consumers' involvement in specifying their security requirements and managing their SMP. The later project fits better with CPs deliver their own services only.

In this paper we introduce a novel approach that tackles both loss of trust and security control problems by enabling CCs to extend their SMP to include cloud hosted assets. Our approach introduces a new cloud security management framework based on aligning the NIST-FISMA standard [12], as one of the main security management standards, to fit with the cloud architectural model. The information required to put the NIST standard into effect is not possessed by one party. Thus we improve the collaboration among the key cloud stakeholders to share such required information. Getting CCs involved in every step of the SMP of their assets mitigates claims of loosing trust and control. Our approach also mitigates the loss of control claimed by the CPs for the hosted services that are developed by other parties. Being based on a security management standard our approach enables both parties to get security certifications. Our approach helps stakeholders to address the following issues:

- What are the security requirements needed to protect a cloud hosted service given that the service is used by different tenants at the same time?

- What are the appropriate security controls that mitigate the service adoption risks and who select such controls?
- Are the selected controls available on the cloud platform or we will/can use third party controls?
- What are the security metrics required to measure the security status of our cloud-hosted services?

To validate our approach we developed a prototype of our collaboration-based cloud security management framework and deployed it on a cloud platform hosting a SaaS application (an ERP Service). We evaluated the approach by securing the ERP service assuming that the cloud platform has multiple tenants sharing the same cloud application. Each tenant has their own security requirements and SMP.

In section II we use a motivating scenario to highlight the research problems we aim to address. Then we give an overview of cloud computing security issues and the SMP. Section III reviews related work in cloud computing security research areas. Section IV discusses our approach and security standards used. Section V describes our framework architecture. Section VI explains a usage example of the developed framework. In Section VII we discuss the implications of our work and further research.

II. MOTIVATION

A. A Motivating Example

Swinburne University is going to purchase a new Enterprise Resource Planning (ERP) solution in order to improve its internal process. After investigation, Swinburne decided to adopt the Galactic ERP solution (a cloud-based solution), to save upfront hardware investment required and to optimize infrastructure costs. Galactic is a Web-based solution developed by SWINSOFT. SWINSOFT hosts its applications on a cloud platform delivered by GREENCLOUD (GC). GC delivers IaaS and PaaS. SWINSOFT uses third party services to accelerate the development process. Such services are developed by GC and deployed on the GC platform including: (1) Workflow-Builder service (customizable workflow management service), (2) Currency-Now service (retrieves the current exchange rate of currencies), (3) Batch-MPRD (used in posting operations based on the map-reduce model). At the same time, Auckland University has the same interest in using the Galactic ERP solution, as shown in Figure 1. Swinburne and Auckland are security certified. *Swinburne* needs to maintain a similar security level on Galactic as applied on their internal IT systems. *Auckland* assigns high risk impact to the Galactic asset. Thus each stakeholder has different security constraints to enforce on the same service.

B. The Cloud computing model security problem

The cloud model has different dimensions that participate in complicating its security problem including [2]:

1) The model has different Service Delivery Models (SDMs): Infrastructure as Service (IaaS), Platform as Service (PaaS), and Software as Service (SaaS). Each SDM has different possible implementations (SaaS may be hosted on top of PaaS or IaaS) and its own security issues based on the underlying technology. Accordingly each SDM has a set of security controls that are required to mitigate such issues.

2) The cloud model has two key characteristics: *Multi-tenancy* which results in virtualzing the boundaries among the hosted services of different tenants, and *elasticity* which requires secure services' migration and placement strategies.

3) The model has a long stack of dependent layers where the security of each layer depends on lower layers' security.

4) The model has different stakeholders involved including CPs, SPs, and CCs. Each stakeholder has their own security needs that may conflict with other stakeholders' needs.

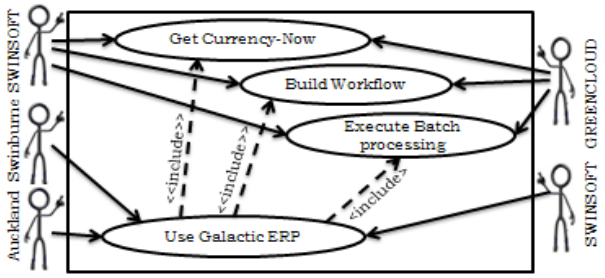

Figure 1: A use case diagram for the motivating example

C. Information Security Management Systems

Information security management systems (ISMS) are defined in ISO27000 as [6] "*systems that provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the protection of information assets.*". These operations are grouped into three main phases:

1) Defining security requirements - this phase includes (i) identifying security goals/objectives that the ISMS should satisfy and deliver, (ii) conducting risk analysis and assessment to identify existing risks within the system scope, and (iii) detailing objectives/risks into detailed security requirements and security policies.

2) Enforcing security requirements - this phase includes: (i) identifying security controls to be used, and (ii) implementing and configuring such controls based on the specified security requirements.

3) Monitoring and Improving security - this phase includes (i) monitoring the current status of the implemented security controls, (ii) analysing the measured security status to identify existing security issues, and (iii) maintaining and improving the current security controls.

D. Key challenges

After analyzing the cloud computing model security problem, the ISMS process, and the motivating scenario we have identified the following key problems:

1) Each stakeholder has their own SMP that they want to maintain/extend to the cloud hosted assets.
2) No stakeholder can individually maintain the whole security process of the cloud services because none of them has the full information required to manage security and each one has a different perspective.

3) Multi-tenancy requires maintaining different security profiles for each tenant on the same service instance.
4) No Security SLA is available that can be used to maintain agreements related to cloud assets security.
5) The existing standards such as ISO27000 and FISMA do not map well to the cloud model because these standards consider the SMP from the platform/asset owner not from a Service Provider perspective.

E. Key requirements of the cloud ISMS

Any proposed security management framework for the cloud model should cover the following key requirements:

1) Enable CCs to specify their security requirements on the cloud hosted assets and the underlying cloud platform.
2) Enable CCs to monitor their assets security status and the underlying platform security status as well.
3) Support for multi-tenancy where different tenants can maintain their SMP with strong isolation of data.
4) Be based on existing security management standards that are already adhered by the CCs and CPs.

III. RELATED WORK

A. Cloud security engineering

Menzel et al [7, 8] proposed a model driven approach and a language to specify security requirements on web services and cloud web applications composed of web services. Each application instance (and its services) is deployed on a VM. They assumed that (1) web applications are composed of web services only, (2) multi-tenant security is maintained through using VMs for each tenant (simplest case), and (3) the underlying infrastructure security is not considered. Bertram et al [9] proposed a similar idea of security engineering for cloud hosted services with more higher level of abstraction (risk-based instead of security-requirements-based). The authors assumed a trusted and secured cloud platform with a focus to provide security PaaS that can manage and mitigate security risks of the services shared among two collaborating enterprises. Both efforts cover only Web services and capture/generate security on the service level without considering the underlying layers.

B. Cloud security management

Saripalli et al [10] proposed a quantitative risk analysis and assessment method based on NIST- FIPS-199 [5]. Risk assessment is a step in the SMP. The remaining steps of the SMP are still required. Although the authors proposed a quantitative method in assessing risks, they used qualitative evaluation bands (Low, Medium, and High). Similar efforts were carried out by Xuan et al [11]. ISO27000 [6], NIST-FISMA [12] are the two main ISMS standards. Both standards do not fit well with the cloud model because they assume that asset owner has full control over the SMP of his assets (hosted inside enterprise boundaries). Moreover, they do not consider the scenario of sharing a service "Multi-tenancy" among consumers. Related research efforts in ISMS include risk assessment and management frameworks such as OCTAVE [13], CORAS [14], Security management systems such as policy-based security management [15], Ontology-based and policy based management has been merged in one approach [16], and model-based security management [17]. Most of these approaches focus on the security capturing and enforcement phases rather than the feedback and improvement phases of the SMP. These phases become more critical in the cloud model because we moved from security within enterprise boundaries to securing assets hosted on third-party platforms.

C. *Cloud Security SLA management*

Security SLA is another approach to specify and manage security. Although a lot of proposals have been introduced in SLA management (SLA specification, enforcement and monitoring), security is rarely considered as it's different from the other QOS attributes such as performance and reliability. Shirlei et al [18] focused on Sec-SLA objectives related to data backup policy only. Pankesh et al [19] has proposed a cloud SLA management architecture but security is not covered. A reasonable justification of the lack of Sec-SLAs is the difficulty in defining suitable security metrics.

IV. OUR APPROACH

Our approach is based on improving and supporting collaboration among cloud stakeholders to develop a cloud security specification and enforcement covering all of their needs. Our approach is based on aligning FISMA standard with the cloud model and utilizing collaboration among the stakeholders to maintain a cloud security specification covering their needs. We first illustrate how we aligned the FISMA standard to fit with the cloud computing model.

A. Aligining NIST-FISMA standard with the cloud model

The Federal Information Security Management Act **(**FISMA) standard [20] defines a framework for managing the security of information and information systems that support the operations of the agencies. The framework has six main phases including: service security categorization, security controls selection, security controls implementation, security controls assessment, service authorization, and security monitoring. Table 1 summarizes how we aligned FISMA model to fit with the cloud model.

(1) Service Security Categorization - Each service (S_J) on the cloud platform can be used by different tenants. Each service tenant (T_i) owns their information only the shared service ($S_{J)}$. The tenant is the only entity that can decide/change the impact of a loss of confidentiality, integrity and availability on their business objectives. Each tenant may assign different impact levels (Low, Medium, or High) to security breaches of their information. In FedRAMP [4], the CP specifies the security categorization of services delivered on their cloud platform. However, this is not sufficient as the CP does not have sufficient knowledge about the impact of information security breaches on their tenants' business objectives.

Table 1: Alignment of NIST-FISMA standard with the cloud computing model

Phase	Task	CP	SP	CC	Inputs	Outputs
Security categorization	Categorize security impact (SC)	Informed	Informed	Responsible	Business objectives	Security Impact Level
Security controls selection	Register security controls	Responsible	Responsible	Responsible	Control Datasheet	Security controls registry
	Generate security controls baseline	Responsible (Automated by the framework)			Service SC + Controls registry	Controls baseline + matching status
	Assess service risks	Responsible			Service + platform arch. + service CVEs + CWE	Service Vulnerabilities + Threats + Risks
	Tailor security baseline	Responsible			Baseline + Risk assessment	Security mgmt plan (Sec-SLA)
controls implementation	Implement security controls	Responsible			Security mgmt plan	Updated Security plan
Security Assessment	Define security metrics	Responsible	Informed	Responsible	Security objective	Security assessment plan
	Assess security status	Responsible (Automated by the framework)			Security assessment plan	assessment report
Service Authorization	Authorize service	Informed	Informed	Responsible	Security plan + assessment report	Service authorization
Security Monitoring	Monitor security status	Responsible (Automated by the framework)			Security assessment plan	Security status report

Our approach enables CCs to be involved in specifying the security categorization of their information. Moreover, our approach enables both scenarios where we can consider the security categorization (SC) per tenant or per service.

The security categorization of the service is calculated as the maximum of all tenants' categorizations:

$$SC(T_i) = \{(\text{confidentiality, impact}), (\text{integrity, impact}), (\text{availability, impact})\},\ \text{Impact} \in \{\text{Low, Medium, High}\} \quad \text{Eq. (1)}$$

$$SC(S_j) = \{(\text{Confidentiality, Max}(\forall T_i(\text{impact})), (\text{Integrity, Max}(\forall T_i(\text{impact})), (\text{Availability, Max}(\forall T_i(\text{impact}))\} \quad \text{Eq. (2)}$$

(2) Security Control Selection - The selection of the security controls to be implemented to protect such assets from being breached has two steps: (a) baseline security controls selection. The FISMA standard provides a catalogue of security control templates categorized into three baselines (low, medium and high). Based on the security categorization of the tenant or the service we can select the initial baseline of controls that are expected to provide the required level of security specified by tenants; (b) Tailoring of the security controls baseline. We tailor the security controls baseline identified to cover the service possible vulnerabilities, threats, risks and the other environmental factors as follows:

I. The service risk assessment process

- *Vulnerabilities Identification* - this step requires being aware of the service and the operational environment architecture. We consider the involvement of the SP who knows the internal structure of the provided service and the CP who knows the cloud platform architecture.
- *Threat Identification* - the possible threats, threat sources and capabilities on a given service can be identified by collaboration among the SPs, CPs, and CCs. CCs are involved as they have the knowledge about their assets' value and know who may be a source of security breaches.
- *Risk Likelihood* - based on the capabilities of the threat sources and the nature of the existing vulnerabilities, the risk likelihood is rated as low, medium or high.
- *Risk Level (Risk Exposure)* - based on the risk impact (as defined in phase 1) and risk likelihood we drive the risk level as (Risk Level = Impact X Likelihood).

II. The security controls baseline tailoring process

Based on the risk assessment process, the selected security controls baseline is tailored to mitigate the new risks and to fit with the new environment conditions as follows:

- *Scoping of the Security Controls:* (i) Identify the common security controls; The cloud stakeholders decide on which security controls in the baseline they plan to replace with a common security control (either provided by the CPs or by the CCs), (ii) Identify critical and non-critical system components; the SPs and CCs should define which components are critical to enforce security on it and which are non-critical (may be because they are already in a trusted zone) so no possible security breaches, and (iii) Identify technology and environment related security controls that are used whenever required such as wireless network security controls.
- *Compensating Security Controls* - whenever the stakeholders find that one or more of the security controls in the tailored baseline do not fit with their environment conditions or are not available, they may decide to replace such controls with a compensating control.
- *Set Security controls parameters* - the last step in the baseline tailoring process is the security controls' parameters configuration, such as minimum password length, max number of unsuccessful logins, etc. This is done by collaboration between the CPs and CCs.

The outcome of this phase is a security management plan that documents service security categorization, risks, vulnerabilities, and the tailored security controls baseline.

(3) Security Controls Implementation - The security plan for each tenant describes the security controls to be

implemented by each involved stakeholder based on the security control category (common, service specific). The common security controls implementation is the responsibility of the common control provider who may be the CPs (in case of internal security controls) or the CC (in case of external controls). The service-specific security controls implementation is the responsibility of the SPs. Each stakeholder must document the security controls implementation configurations in the security mgmt plan.

(4) Security Controls Assessment - Security controls assessment is required to make sure that the security controls implemented are functioning properly and meet the security objectives specified. This step includes developing a security assessment plan that defines what are the controls to be assessed, what are the assessment methods to be used, and what are the security metrics for each security control. The results of the assessment process are documented in a security assessment report. This step may result in going back to the previous steps in case of deficiency in the controls implemented or continuing with the next steps.

(5) Service Authorization - This step represents the formal acceptance of the stakeholders on the identified risks involved in the adoption of the service and the agreed on mitigations. The security plan and security assessment plan are the security SLA among the involved parties.

(6) Monitoring the Effectiveness of Security Controls - The CPs should provide security monitoring tools to help the CCs in monitoring the security status of their assets. The monitoring tools should have the capability to capture the required security metrics and report the collected measures in a security status report either event-based or periodic-based. The results of the monitoring process may require re-entering the SMP to handle new unanticipated changes.

B. Security automation

After aligning the FISMA standard with the cloud model we adopted a set of security standards to help improving the framework automation and its integration with the existing security capabilities, as shown in Figure 2 and Table 2.

Common Platform Enumeration (CPE) [21] -The CPE provides a structured naming schema for IT systems including hardware, operating systems and applications. We use the CPE as the naming convention of the cloud platform components and services. This helps in sharing the same service name with other cloud platforms and with the existing vulnerabilities databases - NVD [22].

Common Weakness Enumeration (CWE) *and* ***Common Attack Pattern Enumeration and Classification (CAPEC)*** [21] - The CWE Provides a catalogue of the community recognized software weaknesses. The CAPEC provides a catalogue of the common attack patterns. Each attack pattern provides a description of the attack scenario, likelihood, knowledge required and possible mitigations. We use the CWE and CAPEC as a reference for the cloud stakeholders during the vulnerabilities identification phase.

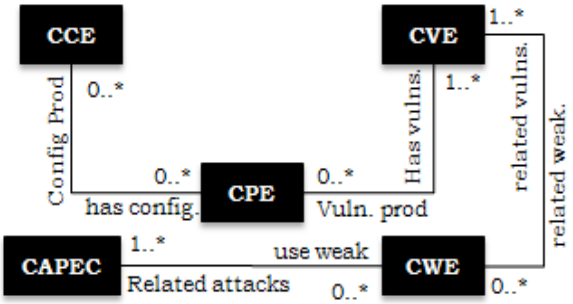

Figure 2: A class diagram of the adopted security standards

Common Vulnerability and Exposure (CVE) [21] - The CVE provides a dictionary of the common vulnerabilities with a reference to the set of the vulnerable products (encoded in the CPE). It also offers vulnerability scoring that reflects the severity of the vulnerability. We use the CVE to retrieve the know vulnerabilities discovered in the service or the platform under investigation.

Common Configuration Enumeration (CCE) [21] - The CCE provides a structured and unique naming to systems' configuration statements so that systems can communicate and understand such configurations. We use the CCE in the security controls implementation phase. Instead of configuring security controls manually, the administrators can assign values to security control templates' parameters. Our framework uses these configurations in managing the selected security controls.

Table 2: Formats of the adopted security standards

Standard	Format	Example
CPE	cpe:/ {part} : {vendor} : {product} : {version} : {update} : {edition} : {language}	cpe:/a:SWINSOFT: Galactic:1.0: update1:pro:en-us
CVE	CVE-Year-SerialNumber	CVE-2010-0249
CWE	CWE-SerialNumber	CWE-441
CAPEC	CAPEC-SerialNumber	CAPEC-113
CCE	CCE-softwareID-SerialNumber	CCE-17743-6

V. CLOUD SECURITY FRAMEWORK ARCHITECTURE

Our framework architecture consists of three main layers: a management layer, an enforcement layer, and a feedback layer. These layers, shown in Figure 3, represent the realization of the ISMS phases described in section II.

Management layer. This layer is responsible for capturing security specifications of the CPs, SPs, and CCs. It consists of: (a) The security categorization service used by the hosted services' tenants to specify security categorization of their information maintained by the cloud services; (b) The collaborative risk assessment service where all the cloud platform stakeholders participate in the risk assessment process with the knowledge they posses. (c) The security controls manager service is used to register security controls, their mappings to the FISMA security controls' templates, and their log files structure and locations. (d) The security metrics manager service is used by the cloud stakeholders to register security metrics they need to measure about the platform security. (e) The multi-tenant

security plan (SLA) viewer service is used to reflect the tenant security agreement. This shows the tenant-service security categorization, vulnerabilities, threats, risks, the selected mitigation controls and the required metrics. (f) The multi-tenant security status viewer. This reflects the current values of the security metrics and their trends.

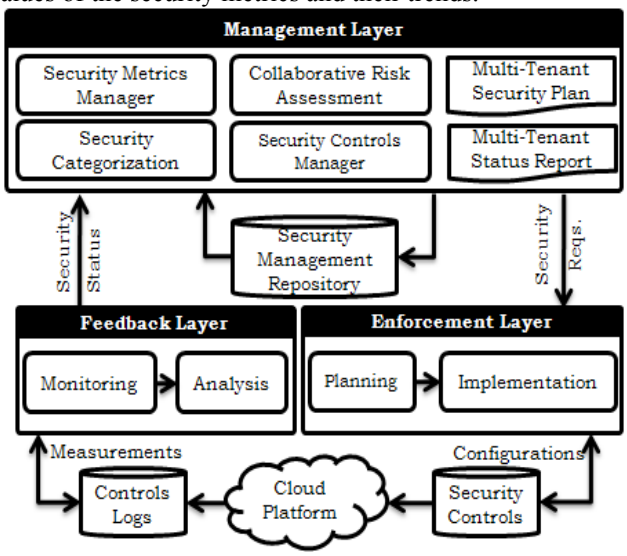

Figure 3: The collaboration-based framework architecture

Enforcement layer. This layer is responsible for security planning and security controls selection based on the identified risks. The selected security controls are documented in the security management plan. The implementation service then uses this plan for maintaining security control configuration parameters and the mapping of such parameters to the corresponding security controls.

Feedback layer. This layer has two key services: the monitoring service which is responsible for collecting measures defined in the security metrics manager and storing it in the security management repository to be used by the analysis service and by the multi-tenant security status reporting service. The analysis service analyses the collected measures to make sure that the system is operating within the defined boundaries for each metric. If there is a deviation from the predefined limits, the analysis service will give alerts to update the current configurations.

VI. USAGE EXAMPLE

To demonstrate the capabilities of our cloud computing security framework and our prototype tool implementing this framework we revisit the motivating example from section II, a cloud based ERP system "Galactic" used by Swinburne and Auckland (CCs), developed by SWINSOFT (SP), and deployed on the GC (CP). The two tenants using the Galactic ERP services, Swinburne and Auckland, are still concerned about their assets' security on the cloud. Both have their own SMP and their own security requirements to be enforced on their cloud assets.

The first step in our approach is to register the Galactic ERP service in the cloud platform service repository so that it can be used by the CCs. This step can be done either by SWINSOFT or by the GC. In this step we use the CPE name as the service ID, Figure 4 (top). A new tenant, Auckland, can register their interest in using the Galactic service. Then Auckland will be granted a permission to manage the security of his information maintained by Galactic service. The same is done by Swinburne, Figure 4 (bottom).

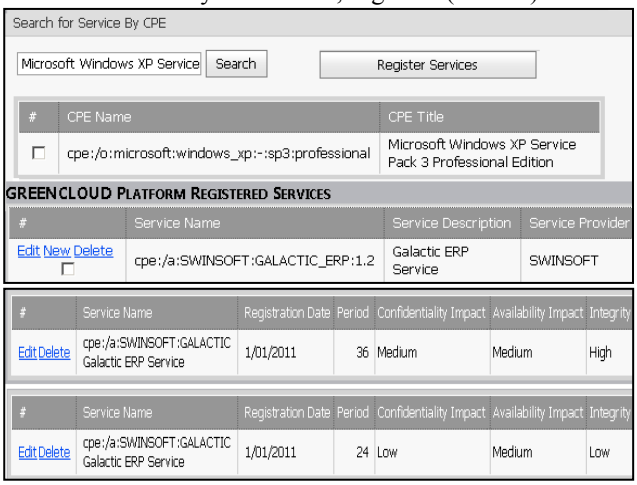

Figure 4: Registering a service (top) and tenants (bottom)

Now Auckland and Swinburne can use our framework to maintain their SMP on their assets as follows:

1) *Service Security Categorization*: The Swinburne security administrator specifies the impact level of losing the confidentiality, integrity, and availability of their data maintained by the Galactic ERP service. The same will be done by the Auckland security administrator, as shown in Figure 4 (bottom). Whenever a new tenant registers their interest in a service and defines their security categorization of data processed by the service (or any of the existing tenants update his security categorization), the framework will update the overall service security categorization.

2) *Security Controls Selection*: The GC as a cloud provider already publishes their security controls database. Swinburne and Auckland can register their own security controls using the security controls manager service. Based on the security categorization step, the framework generates the security controls' templates baseline. This baseline identifies the security controls' templates that are: **satisfied** (matches one of the registered security controls), **missing** (does not match registered security controls), and **duplicate** (more than one matched control), shown in Figure 5.

a. The Service Risk Assessment Process. Galactic vulnerabilities are identified for the first time by SWINSOFT with the help of GC who know the architecture of the service and the hosting cloud platform. Both SWINSOFT and GC have the responsibility to maintain the service vulnerabilities list up to date. The framework enables to synchronize the service vulnerabilities with the community vulnerabilities database - NVD. Each CC – Swinburne and Auckland – should review the defined threats and risks on Galactic and append any missing

threats. The framework integrates with the CWE and CAPEC databases to help stakeholders in identifying possible vulnerabilities whenever the service does not have vulnerabilities recorded in the NVD.

#	Ctl Family	Ctl No.	Enhancement	Ctl Name	Control Status
Edit Delete	AC-	14	1		Missing
Edit Delete	AC-	17	1	Authenitcator	Available
Edit Delete	AC-	17	1	SwinAntiVirus	Duplicate
Edit Delete	AC-	17	2	Authenitcator	Available
Edit Delete	AC-	17	2	SwinAntiVirus	Duplicate

Figure 5: Security controls baseline with controls' status

The Security Management plan for the service: Galactic ERP Service

#	Registration Date	Registration (Mths)	Security Categorization
	1/01/2011	24	Low

Vulnerability Name	Vulnerability Description
CVE-2005-0413	Multiple SQL injection vulnerabilities in MyPHP Forum 1.0 allow remote attackers to execute arbitra
CVE-2005-2471	pstopnm in netpbm does not properly use the "-dSAFER" option when calling Ghostscript to convert a
CVE-2005-4195	Multiple SQL injection vulnerabilities in Scout Portal Toolkit (SPT) 1.3.1 and earlier allow remote

Threat Name	Threat Description	Threat Source
DenialSrv	Denial of service	Attacker
InfoCopy	Copy of information at storage	Internal
InfoMod	Modification of information while being transfered	Attacker
MemMod	Modification of data being processed	Maleware

Risk Name	Risk Probability	Confidentiality Impact	Availability Impact	Integrity Impact	Risk Level
DOS	0.7	Low	High	Low	Medium

Control Name	Control Description	Control Baseline	Control Type	Control Family
Authenitcator	an authenitcation security control	Low	Specific	Access Control
SwinAntiVirus	an antivirus security solution	Low	Common	System and Information Integrity
SwinIPS	an intrusion prevention system	Low	CommonControl	System and Information Integrity

Measurement Name	Measurement Description	Frequency	Measrement Steps	Security Control
LoginActivity	Identify the user login rates	48	count(logstatus)	Authenitcator

Figure 6: Auckland security management plan

b. The controls baseline tailoring process. The CCs decide which security controls in the baseline they plan to replace with common security controls provided by the CP or the CC, as shown in Figure 5. Then SWINSOFT, Auckland, and Swinburne select the critical service components that must be secured. Swinburne and Auckland define their security controls' parameter configurations. The security controls provided by the cloud platform can only be reviewed.

The final outcome of this step is a security management plan that documents the service security categorization, vulnerabilities, threats, risks, and the tailored security controls to mitigate the identified possible security breaches, as shown in Figure 6.

3) *Security Controls Implementation:* *Each stakeholder* implements the security controls under their responsibility as stated in the security plan and the security controls configurations as specified in the previous step.

4) *Assessing the implemented security controls*: The controls to be assessed and the objectives of the assessment are defined by GC, Auckland and Swinburne and documented in the tenant security assessment plan. The execution of such plan, the assessment process, should be conducted by a third party. Our framework helps in assessing security controls status when using security controls that integrate with our framework (the framework can understand and read their log structure). The outcome of the assessment phase is a security assessment report.

5) *Service Authorization:* Swinburne and Auckland give their formal acceptance of the security plan, assessment plan, and the assessment reports. This acceptance represents the authorization decision to use Galactic by the CC.

6) *Monitoring the effectiveness of the security controls*: The framework collects the defined security metrics as per the assessment plan of each tenant and generates status reports to the intended cloud stakeholders. A report shows the metrics status and trends, as shown in Figure 7.

Measurement Name	Measurement Date	Measurement Value
LoginActivity	12/01/2011	8
LoginActivity	13/01/2011	10
LoginActivity	14/01/2011	14
UnsuccessfulLogins	10/01/2011	2
UnsuccessfulLogins	11/01/2011	4
UnsuccessfulLogins	12/01/2011	6
UnsuccessfulLogins	13/01/2011	8

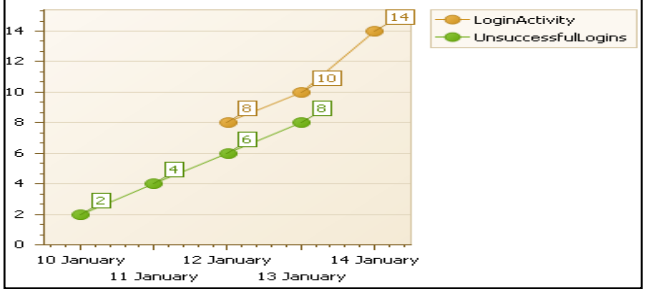

Figure 7: Sample of Swinburne security status report

VII. DISCUSSION

The procedure we went through in the example above should be applied not only for published services but also on the cloud platform services themselves. In this case the CP uses our framework to manage the platform security from a consumer perspective. We have done this for the Galactic exemplar used above.

Our approach provides a security management process; a set of standards-based models for describing platforms, platform services, and services; the security needs of different stakeholders; known threats, risks and mitigations for a cloud deployment; and a tool supporting security plan development and partial automation of a derived security plan. Our approach is comprehensive, supporting all stakeholder perspectives, and collaborative, allowing different stakeholders to develop a mutually-satisfying security model. It addresses the multi-tenancy nature of shared cloud-hosted services when tenants have different security requirements and different SMPs. This is achieved by maintaining and managing multiple security profiles with multiple security controls on the same service. Such controls are delivered by security vendors. This also enables managing traceability between controls, the identified risks and identifies what are the risks still not mitigated.

The SMP of a cloud service has two possible scenarios: Either to let each tenant go through the whole SMP as if he is the only user of the service (tenant-based SMP) or to accumulate all tenants security requirements on a given service and maintain the SMP on the service level (service-based SMP). The later scenario is more straight forward because cloud stakeholders collaborate together to secure the cloud platform and their services with one set of security requirements. The former scenario gives the CCs more control in securing their cloud hosted asset but it has the following problems: (i) the current multi-tenancy feature delivered by the cloud services enables tenants to customize service functionality but it does not enable tenants to customize service security capabilities; (ii) the underlying cloud platform infrastructure, such as OS, does not support for multi-tenancy, so we cannot install multiple anti-viruses or anti-malware systems on the same OS while being able to configure each one to monitor specific memory process for a certain user. One solution may be to use a VM for each tenant as in [7]. This work around may not be applicable if the service is not designed for individual instances usage or if the cloud platform does not support VM technology.

Whenever the CCs are not interested in following the security standards or require a light-weight version of our approach, they can leave out as many steps as they want including security controls implementation, security assessment and service authorization steps. The mandatory steps are service categorization and controls selection. Another variation of our framework is to enable CPs to deliver predefined security versions for the service. CCs can select the suitable version based on their security needs.

We are exploring the cloud security engineering and security controls development processes to develop more flexible services to fit with cloud requirements. Our framework also needs further extension of the automation of the security controls implementation phase. This requires being able to transform from our security plan template configurations into specific security controls configuration. We also plan to derive such configuration parameters' values from the current environment security status.

VIII. SUMMARY

In this paper we introduced a collaboration-based security management framework for the cloud computing model. The framework introduces an alignment of the NIST-FISMA standard to fit with the cloud computing model. We utilize the existing security automation efforts such as CPE, CWE, CVE and CAPEC to facilitate the cloud services Security Management Process (SMP). We have validated our framework by using it to model and secure a multi-tenant SaaS application with two different tenants. The framework can be used by cloud providers to manage their cloud platforms, by cloud consumers to manage their cloud-hosted assets, and as a security-as-a-service to help cloud consumers in outsourcing their internal SMP to the cloud.

ACKNOWLEDGEMENTS

Funding for parts of this research by the FRST SPPI project and Swinburne University of Technology is gratefully acknowledged.

REFERENCES

[1] International Data Corporate (IDC), "*Ranking of issues of Cloud Computing model,"* 2010. <http://blogs.idc.com/ie/?p=730> Accessed Dec 2010.

[2] M. Almorsy, J. Grundy, I. Mueller, "An analysis of the cloud computing security problem," In the proc. of the 2010 Asia Pacific Cloud Workshop, Colocated with APSEC2010, Australia, 2010.

[3] Cloud Security Alliance Group, "*CSA-GRC Stack,"* <www.cloudsecurityalliance.org/grcstack.html>, Accessed Dec'10

[4] *Unofficial FedRAMP Community Collaboration,* http://www.fedramp.net/tiki-index.php, Accessed in Aug 2010.

[5] NIST, "Standards for Security Categorization of Federal Information and Information Systems. *FIPS-199*", <csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199.pdf>, Accessed Dec 2010.

[6] International Organization for Standardization (ISO), "ISO/IEC 27000 - Information technology - Security techniques - Information security management systems - Overview and vocabulary," ISO/IEC 27001:2005(E), 2009, <http://webstore.iec.ch/preview/info_isoiec27000%7Bed1.0%7Den.pdf >, Accessed in July 2010.

[7] M. Menzel, R. Warschofsky, et al, "The Service Security Lab: A Model-Driven Platform to Compose and Explore Service Security in the Cloud," 6th World Congress, SERVICES2010, pp.115-122.

[8] M. Menzel and C. Meinel, "SecureSOA Modelling Security Requirements for Service-Oriented Architectures," IEEE International Conference on Services Computing, 2010.

[9] S. Bertram, M. Boniface, et al., "On-Demand Dynamic Security for Risk-Based Secure Collaboration in Clouds," *IEEE 3rd International Conference* in *Cloud Computing*, pp. 518-525, *2010*.

[10] P. Saripalli and B. Walters, "QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security,", *IEEE 3rd International Conference on Cloud Computing*, 2010, pp. 280-288.

[11] Z. Xuan, N. Wuwong , et al., "Information Security Risk Management Framework for the Cloud Computing Environments," in *2010 IEEE 10th International Conference on Computer and Information Technology (CIT),* 2010, pp. 1328-1334.

[12] NIST, "Risk Management Guide for Information Technology Systems," 2002, <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>, Accessed in June 2010.

[13] P. Marek and J.Paulina, "The OCTAVE methodology as a risk analysis tool for business resources," presented at the International Multiconference Computer Science and IT, Hong Kong, 2006.

[14] R. Fredriksen, M. Kristiansen, et al, "The CORAS Framework for a Model-Based Risk Management Process," in *Computer Safety, Reliability and Security*. vol. 2434, Springer, 2002, pp. 39-53.

[15] C. Basile, A. Lioy, et al, "POSITIF: A Policy-Based Security Management System," in *8th IEEE International Workshop Policies for Distributed Systems and Networks,* 2007, pp. 280-280, Italy.

[16] H. Xu, X. Xia, et al "Towards Automation for Pervasive Network Security Management Using an Integration of Ontology-Based and Policy-Based Approach," 3*rd International Conference Innovative Computing Information and Control*, 2008, pp. 87-87, Dalian.

[17] J. Albuquerque, H. Krumm and P. de Geus, "Model-based management of security services in complex network environments," in *IEEE Network Operations and Management Symposium*, 2008, pp. 1031-1036, Salvador.

[18] S. de Chaves, C. Westphall and F. Lamin, "SLA Perspective in Security Management for Cloud Computing," in *Sixth International Conference Networking and Services*, 2010, pp. 212-217, Mexico.

[19] P. Patel, A. Ranabahu and A. Sheth, "Service Level Agreement in Cloud Computing,", Conference on Object Oriented Programming Systems Languages and Applications, Orlando, Florida, 2009, USA.

[20] NIST, "The Federal Information Security Management Act (FISMA),"U.S. Government Printing 2002,<http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>, Accessed on August 2010.

[21] Mitre Corporation. (2010), *Making Security Measurable*, http://measurablesecurity.mitre.org/, Accessed on Jan 2011

[22] NIST. *National Vulnerabilities Database Home*. http://nvd.nist.gov/, Accessed in Dec 2010.