Collaboration-Based Cloud Computing Security Management Framework
Galactic Case Study

Prepared By
Mohamed Almorsy

January, 2011
# Table of Contents

Table of Contents ............................................................................................................................................................... II

Motivating Scenario .............................................................................................................................................................. 1

1) Register the Galactic-ERP Service ................................................................................................................................. 1
2) Register Tenants for Galactic Service ............................................................................................................................ 2
3) Register security controls ............................................................................................................................................... 3
4) Service Security Categorization .................................................................................................................................. 3
5) Security Controls Selection .......................................................................................................................................... 3
6) Security Controls Implementation ................................................................................................................................. 9
7) Assessing the implemented security controls ............................................................................................................... 9
8) Authorize Service ........................................................................................................................................................... 9
9) Monitoring the effectiveness of the security controls ................................................................................................ 9
10) Screenshots from the Galactic service while operating for the two tenants ......................................................... 10
Motivating Scenario

Swinburne University is going to purchase a new ERP solution in order to improve its internal process. After investigation, Swinburne decided to go for Galactic ERP solution (a cloud-based solution), to save upfront investment required and keep infrastructure cost optimized. Galactic is a Web-based solution developed by SWINSOFT. SWINSOFT hosts its applications on cloud platform delivered by GREENCLOUD (GC). GC delivers IaaS and PaaS. SWINSOFT uses third party services to accelerate the development process. Some of such services are developed and deployed in the GC platform such as: (1) Workflow-Builder service (customizable workflow management service), (2) Currency-Now service (retrieves the current exchange rate of currencies). Other services such as Batch-MPRD (used in posting operations based on the map-reduce model) deployed on BLUECLOUD (BC) platform. On the same time Auckland University has the same interest to go for Galactic ERP solution.

![Use case diagram](image)

Figure 1: A use case diagram for the motivating example

In this scenario we have (1) two CPs: GC and BC, (2) three CCs: Swinburne, Auckland and SWINSOFT, and (3) three SPs: SWINSOFT, GC, and BATCH-MPRD. Swinburne and Auckland are security certified. Swinburne needs to maintain similar security level on Galactic such as ones applied on local systems. Auckland assigns high risk on the Galactic asset, so they have strong security constraints to be enforced.

Now we are going to show how our framework can be used to manage security of the Galactic service for the involved stakeholders.

1) Register the Galactic-ERP Service

The service provider “SWINSOFT” may decide to host Galactic service on a cloud platform “GREENCLOUD” or the cloud provider “GREENCLOUD” may decide that he can offer the Galactic service based on his cloud platform. In both cases they will register the service in the platform service repository so that it can be used by the CCs. This service record is used by the cloud platform management for SLA enforcement and also for our security management framework which can be installed as a plug-in in the cloud management layer. In this step we use the CPE name of the service as a reference, as shown in figure 2-a.
2) Register Tenants for Galactic Service

The next step comes when a new tenant is registered to use one of the published services (Galactic ERP). Then the tenant will be granted a permission to manage the security of the selected service through our framework.

Cloud Security Management Console

Create a New Account

Use the form below to create a new account.

Passwords are required to be a minimum of 6 characters in length.

Account Information

Tenant Name: Auckland

E-mail: admin@auckland.com.au

Password: **********

Confirm Password: **********

Create User

Figure 2-b-1: Auckland Tenant Registration on the cloud platform

Figure 2-b-2: Auckland registers for the Galactic service
3) Register security controls
GREENCLOUD security administrators and CCs – such as Auckland and Swinburne - should define the possible security controls that can be used to enforce the required security. Each control registration should specify the features/functionalties offered by the security control. The registration should also define what are the security controls’ templates (defined by the NIST-FISMA standard) satisfied by this security control.

4) Service Security Categorization
Swinburne security administrator will define 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 (see figure 2-d). Whenever a new tenant registers his interest in a service and defines his 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 (the max. impact value from all tenants).

5) Security Controls Selection
Based on the previous step, the framework generates the security controls’ templates baseline that represents the minimum security requirements that should be enforced based on the specified
tenant/service security categorization. The framework identifies the security controls’ templates **satisfied** (security controls templates that have matching with one of the defined/existing security control), the **missing** (do not have matching with any of the existing actual security control), and **duplicate security controls** (have more than one matched security control) as shown in figure 2-e.

![Figure 2-e: Auckland - Galactic Security Controls baseline](image)

Now we need to tailor the selected security controls baseline to match the expected threats, vulnerabilities and mitigate the missing security controls problem (controls not exist in the baseline) throw compensating controls or using common controls instead of service specific security controls. Below we will explain how the framework helps the cloud stakeholders to manage the above tasks.

- **The risk analysis and assessment process:**

  Galactic vulnerabilities are identified for the first time by SWINSOFT and GC who know the architecture of the service and the cloud platform. Both SWINSOFT and GC have the responsibility to maintain the service vulnerabilities list up to date or select to auto update from the NVD database. Each service consumer – Swinburne and Auckland – will review the defined threats and risks on Galactic and appends the missing threats and/or risks. The framework provides stakeholders with the CVE vulnerabilities database – NVD. So they can retrieve recently discovered vulnerabilities in Galactic service or the underlying platforms by the community. The framework also provides the stakeholders with a CWE and CAPEC databases. So they can use as a reference during the risk assessment phase.
Figure 2-f-1: CWE dictionary used by stakeholders in the risk assessment phase

Figure 2-f-2: CWE dictionary used by stakeholders in the risk assessment phase
The security controls baseline tailoring process:

(a) Scoping of security controls:

(i) Identify common security controls. GC already publishes their security controls currently implemented. At the same time, Swinburne and Auckland has their own common security controls. So they will need to register it first (using the security controls manager). Then the stakeholders decide on what security controls in the baseline they plan to replace with common security controls from both sides (see figure 2-g).
(ii) Identify critical and non-critical system components: SWINSOFT, Auckland, and Swinburne select the critical service components that must be secured.

(iii) Technology, regulation, and environment related security controls. We did not use it in our example. But it’s still doable using the same functionality as shown in figure 2-g.

(b) Compensating Security Controls

The stakeholders can replace security controls in the baseline using the security controls mapping tool where they can add or remove security controls from the tailored controls list, as shown in figure 2-g.

In this step let’s assume that Swinburne selected to use forms authentication delivered by the galactic service while Auckland decided to use their SSO to depend on their active directory. We will see this implication in the operation of the service after implementing the selected security control, see figure 2-m.

(c) Set Security controls parameters
Swinburne and Auckland define their security controls’ parameters configurations. In the case of common controls used from the cloud platform we can only inherit these values but cannot override it, as shown in figure 2-i.

![Figure 2-i: Setting security controls parameters](image)

The 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 2-j.

![Figure 2-j: The security management plan for Auckland tenant (Sec-SLA)](image)
6) Security Controls Implementation
Each tenant - Swinburne and Auckland - should implement the common security controls under their responsibility as stated in the security management plan and the security controls configurations as shown in figure 2-i.

7) Assessing the implemented security controls
The controls to be assessed and the objectives of the assessment are defined by all our stakeholders (GC, SWINSOFT, Auckland and Swinburne) and documented in the security assessment plan as shown in figure 2-k. The execution of such plan (the actual assessment process) should be conducted by a third party the currently known assessor specialized in NIST-FISMA is the FedRAMP project. The framework can help in assessing security controls status in case of using security controls that integrate with the framework. The outcome of the assessment is the security assessment report which should look like the report in figure 2-l. Now we may go back to step 2 or 3 (in case of any deficiency discovered in the assessment report), or continue to the next step.

8) Authorize Service
Swinburne and Auckland should confirm their formal acceptance of the security management plan, security assessment plan, and the security assessment reports. This acceptance represents the authorization decision to start using Galactic by the CC.

9) Monitoring the effectiveness of the security controls
The framework collects the defined measures as per the configured frequencies (for each tenant) and send it in a status report form to the intended cloud stakeholders. The report shows the current
values of the defined measures and there trend. This will help the tenants’ administrators in improving their security status and detect attacks or system weaknesses (see figure 2-m).

<table>
<thead>
<tr>
<th>Measurement Name</th>
<th>Measurement Date</th>
<th>Measurement Results</th>
<th>Measurement Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LoginActivity</td>
<td>12/01/2011</td>
<td></td>
<td>15</td>
</tr>
<tr>
<td>LoginActivity</td>
<td>13/01/2011</td>
<td></td>
<td>18</td>
</tr>
<tr>
<td>LoginActivity</td>
<td>14/01/2011</td>
<td></td>
<td>1650.0</td>
</tr>
<tr>
<td>UnsuccessfulLogins</td>
<td>10/01/2011</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>UnsuccessfulLogins</td>
<td>11/01/2011</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>UnsuccessfulLogins</td>
<td>12/01/2011</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>UnsuccessfulLogins</td>
<td>13/01/2011</td>
<td></td>
<td>6</td>
</tr>
</tbody>
</table>

Figure 2-m: security status report for one tenant – Auckland

10) Screenshots from the Galactic service while operating for the two tenants
Recall that Swinburne is using the forms-based authentication offered by the Galactic service and Auckland is using SSO with a link to their active directory, as shown in figure 2-n below.

a) One of the users of Swinburne is trying to connect so he got authenticated using login form as below:
b) One of the users of Auckland is connected. He is authenticated using SSO as below:
c) A sample of the authenticator control log file is shown in the below figure:

```xml
<LogFile xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <LogEntry>
    <UserName>C11</UserName>
    <UserIPAddress>192.168.1.2</UserIPAddress>
    <logstatus>success</logstatus>
  </LogEntry>
  <LogEntry>
    <UserName>C11</UserName>
    <UserIPAddress>192.168.1.3</UserIPAddress>
    <logstatus>failed</logstatus>
  </LogEntry>
  <LogEntry>
    <UserName>C11</UserName>
    <UserIPAddress>192.168.1.4</UserIPAddress>
    <logstatus>failed</logstatus>
  </LogEntry>
</LogFile>
```

d) Figure 2-n-4: Sample of the authenticator control log file