Strategic Analysis of Compliance, Governance and Security for Sales force

T. Geetha Lakshmi[1]
Assistant Professor
Computer science and Engineering College
CMR College of Engineering and Technology
Kandlakoya, Medchal, Secunderabad.

M. Kavitha[2]
Assistant Professor
Information Technology College
CMR Engineering College
Kandlakoya, Medchal, Secunderabad

Abstract Sales force is one of major leading CRM (Customer Relationship Management) software which is benefits from cloud. It has more than 1000's applications to support various features like generating new leads, acquiring new leads, increasing sales and closing the old deals. It is designed to manage the organization's data focused on customer related application and sales related details. It also offers features to personalize its native data structures and GUI to suit the specific needs of a business. More recently, it has started offering the IOT (internet of things) connectivity to the CRM platform. Large companies have established policies for corporate governance, and many others follow security policies to safeguard consumer or financial information. This paper we focus on Sales force Data, Metadata, and Tooling API to generate powerful reports that help achieve better compliance, governance, and security. Sales force Shield provides additional native capabilities and other useful services.

Keywords: CRM, Sales force , Compliance, Governance and Security

I. Introduction

The Salesforce Application Governance Method (SAGM) is designed to help organizations meet their strategic and tactical goals in utilizing the Force.com platform. The SAGM can support the full spectrum of development activity on the Force.com platform and is suitable for the needs of a Citizen Developer through to the needs of a Service Integrator that has large teams of developers. The goal of the SAGM is to enable an organization to be assured that all development activity taking place on the Force.com platform is done in a consistent manner and to a consistent set of standards. This is not to say every developer will produce exactly the same solution given a common set of requirements. It does however mean that there is consistency in the structure and usage of the platform so that the same "rules" apply to anyone using the platform to deliver business value. This goal is important because over time, without a clear set of standards developers will follow their own rules, and the more developers that create applications that way; the higher amount of technical debt that will be built up, to the point where applications may be deployed and no one really has a clear understanding of what it does and why.

The SAGM utilizes 9 phases to provide coverage of the Force.com platform. Each phase is consistent in its approach. As this is a method, it is possible to simply reference the Phase directly that relates to the area that requires governance.

The 9 phases are as follows:
A – Application Architecture
B – Data Architecture & Management
C – Identity & Access Management
D – Sharing & Visibility
E – Integration
F – Apex, Visual force & Lightning
G – Communities
H – Mobile Solutions Architecture
I – Development Lifecycle & Deployment

These phases loosely relate to the Path taken by a Salesforce Certified Technical Architect (CTA), providing synergy between the educational path to understanding the Salesforce platform and the ability to govern it.

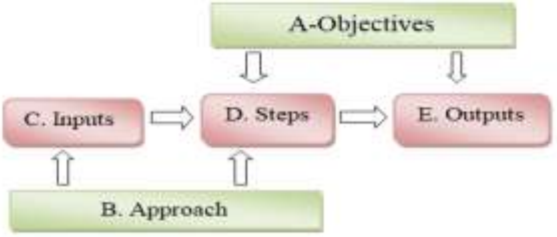

Fig:- phase level

As previously mentioned, the SAGM is designed to be referenced directly at the phase level (i.e. the Phase that is currently being governed), so in that respect there is a consistency in the way each phase has been documented. The following diagram provides an overview of that structure.

The following provides a definition of the elements that define the phase structure.

Method	Description
A- Objectives	A specific result that the Phase aims to achieve In general, objectives are more specific and easier to measure than goals. Objectives are basic tools that underlie all planning and strategic activities.
B- Approach	A recommendation as to how the Phase will be implemented and/or executed.

C – Inputs	The artifacts that must be available before the Phase can commence. Artifacts are key inputs into the Phase Steps.
D – Steps	The steps and sub-steps that should be completed for each Phase to determine complete coverage of a project/product from a governance perspective.
E Outputs	The artifacts that will be produced by the Phase and created during the Steps.

Although the phases clearly state what needs to be done to govern a solution on the Force.com platform, it is the Resource Base that will be used to determine exactly what standards that governance should use to assess an application.

II. Resource Base

The Resource Base is a set of resources – best practices, tooling, guidelines, templates, checklists and other detailed documents that support each of the SAGM phases. These resources can be used as is, tailored or replaced to meet the project/customer requirements. The resources will underpin the SAGM, therefore it is critical that these resources work within the phases and support the inputs/outputs as detailed in the method

III. Key Points

As a generic method, the SAGM is intended to be used by enterprises in a wide variety of different geographies and applied in different vertical sectors/industry types. As such, it may be, but does not necessarily have to be, tailored to specific needs.

For example:

It may be used in conjunction with the set of deliverables of another framework, where these have been deemed more appropriate for a specific organization. Some of the phases may be deemed as not required, for example the Mobile Solutions Architecture phase if no requirement exists within the organization The order of the phases is intentional, but not fixed. It may be that for certain organizations the order of the phases may change if early warnings are required for specific areas, for example Integration may be a key consideration that requires early assessment before any other phase is considered

IV. Basic Structure

The basic structure of the SAGM is shown in the Salesforce Application Governance Cycle diagram. Throughout the SAGM cycle, there needs to be frequent validation of results against the original expectations, both those for the whole SAGM cycle, and those for the particular phase of the process.

Although an organization is at liberty to adjust the phases, there is a logical order to them. Each Phase takes a more comprehensive and deeper technical view of the application. Given that there is order to the Phases, it is envisaged that each Phase provides the "gate" to proceed to the next Phase.

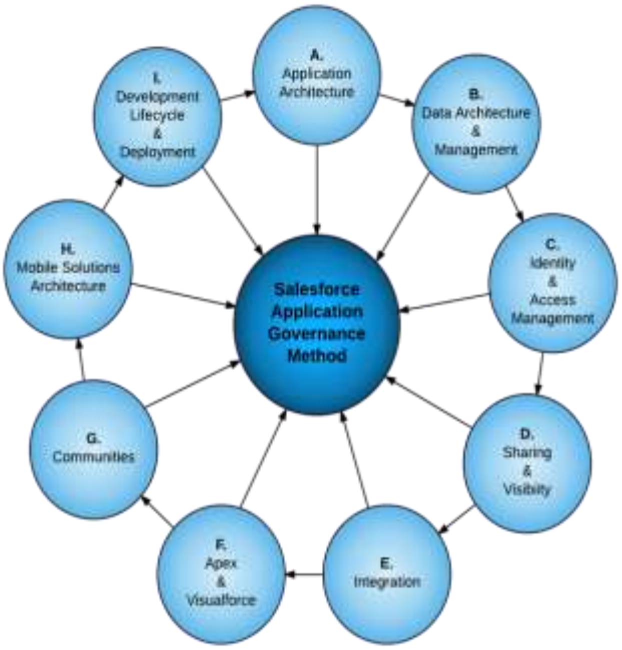
A. Application Architecture
B. Data Architecture & Management
C. Identity & Access Management
D. Sharing & Visibility
E. Integration
F. Apex & Visualforce
G. Communities
H. Mobile Solutions Architecture
I. Development Lifecycle & Deployment
Salesforce Application Governance Method

Fig:- Salesforce Application Governance Cycle

However, this should be a consideration during implementation of the SAGM as some organization will prefer to assess the application in its entirety rather than Phase-by-Phase. Companies achieve better compliance, governance, and security. In most cases, these reports can be assembled with information available from the Salesforce Data, Metadata, and Tooling API. In the last section, you will learn about new sources of information available with Salesforce Shield, including the Event Log File and Field Audit Trail services

V. Essential Reports for Compliance, Governance, and Security

1. Data Dictionary

Custom Objects and Fields are a central focus for any Salesforce account. Between the Data and the Metadata API, there are 70 properties that describe Custom Objects, and a further 80 properties that document Custom Fields. These properties cover everything you can imagine, such as field labels, numeric precision, formula fields, date formats, picklist values, child relationships, and help text. A Data Dictionary can be used to document the current properties for each

Custom Object and Field in a Salesforce account. This is a key compliance report for use by business analysts and application developers interested in documenting the current state of the org. The report could be used by a development team to track project progress, or by a System Integrator before and after a job is completed.

2. Combined Permissions Report

Every user has a Profile that defines what they can see and do. Profile permissions include Application and Tab Visibility, Apex Class and Page Access, Object and Field Permissions, User and Custom Permissions, and Layout Assignments. An administrator can also assign any number of Permission Sets to a user. Permission Sets are similar to Profiles, but are used to grant additional permissions for special situations. A Combined Permissions Report shows how the base Profile and each assigned Permission Set contribute to the actual security permissions for a specific user. This is a key report for security and compliance. For example, a company could document which users have been granted access to fields that contain customer information. In the table below, Permission Sets that changed the base Profile are shown in green, Permission Sets that were not effective are shown in red. This report can be challenging to generate because information from the Data and the Metadata API must be cross-referenced.

3. Record Level Security Report

Profiles and Permission Sets control which objects and fields a user can see. But when it comes to specific records, additional rules apply.

- Salesforce administrators can set up complex record level security rules.
- Every record is owned by a user or a queue. The owner has full access to the record.
- There are organization-wide sharing settings for each object.
- Users higher up in the Role hierarchy have access to the same data as people lower in their hierarchy.
- Manual and programmatic sharing rules create exceptions for particular sets of users.

There is some information on record level access in the Salesforce HTML interface, but only for one record at a time. An effective Record Level Security Report would allow the selection of multiple records and provide detailed information about who has access to each record, what kind of access they have, and why they have the access. This report can help administrators manage sharing rules and document data security.

4. Asset History Report

Think for a second about your production Salesforce account. Most orgs will have Custom Tabs, Page Layouts, Custom Objects, Profiles, Visualforce Pages, and many other configurations. The Metadata API currently supports about 150 different types, and for each type, there are many individual assets. An Unlimited Edition org can have up to 2000 Custom Objects, each with a maximum of 500 fields. There can be hundreds or even thousands of Roles, Profiles, Dashboards, and other assets. Now think about this. Where did all those configurations come from? Who deployed them in the org? Did they flow through the testing Sandbox? Were they modified with the Setup Menu? What was the chain of custody from the developer who created the asset down through various Sandboxes and other staging orgs before it ended up in your production account?

An Asset History Report should be able to answer these questions. Some of this information is tracked by Salesforce, but for the most part this “meta metadata” must be carefully recorded by the change and release management tool that the development team and org administrators are using. This is an essential report for compliance and corporate governance.

5. Metadata Differences Report

An Asset History Report looks at how a Salesforce org was assembled, but additional insights can be gathered by watching how the org has changed over time. Administrators can take periodic metadata snapshots of the org and commit them to a version control system. Then by examining the time-series differences, many interesting questions can be answered. Have Profiles or Permission Sets changed? What new Custom Fields have been added? Did the security configuration change? Have new packages been installed? What Apex Scripts were changed? The Metadata Differences Report provides valuable information for security audits and compliance.

Salesforce Shield

Salesforce Shield adds an additional layer of security to your Salesforce org to help meet complex internal and regulatory compliance requirements. Shield provides some native capabilities, but also some new services that can be used to construct custom reports. The three core services offered by Salesforce Shield are Event Log Files, Field Audit Trail, and Platform Encryption.

The Event Log File custom object provides low-level event logs with all kinds of information relevant to privacy concerns, security situations, and data exfiltration. For example, you can see when Reports are run, Documents are downloaded, Packages are installed, or the Bulk Data API is used. With Field Audit Trail you can specify a retention policy for field history and retain archived data for up to 10 years. Lastly, Platform Encryption can be used to further safeguard data at rest.

6. Activity Timeline Report

This leads on smoothly to finish up with Activity Timeline reporting. The Event Log File and the Field Audit Trail information contain the specific dates of different user activities, along with additional fields that describe the event in more detail. There are other Salesforce objects such as the Setup Audit Trail and Login History that provide related information. Filtering these records by date, an Activity Timeline Report can be constructed that shows every interaction that a user had with Salesforce over a given timeframe.

In the event of a credential-based attack, this report can provide a roadmap of the activities carried out by the attacker. In a data exhilaration event, this report can be used to document the extent of the damage. Rogue administrative actions or accidents can be placed on a timeline. Different activities can be filtered by risk level. The Activity Timeline Report can be used to forensically examine events in the past, or proactively safeguard against future security risks

VI. Conclusion

The SAGM defines a recommended sequence for the various phases and steps involved in governing the development of an application, but it cannot recommend a scope – this is determined by the organization or project. Companies can use the Salesforce Data, Metadata, and Tooling API to generate powerful reports that help achieve better compliance, governance, and security. Salesforce Shield provides additional native capabilities and other useful services. If you see a gap in your compliance and security reporting after reading this post, our Snapshot product can create many of the reports described above and provides additional tools for Change and Release Management.

References

[1] https://appexchange.salesforce.com/listingDetail?listingId=a0N30000003JRPTEA4&tab=r

[2] https://compliance.salesforce.com/en

[3] https://www.salesforce.com/solutions/industries/government/compliance/

[4] https://www.skyhighnetworks.com/cloud-security-blog/compliance-governance-and-salesforce-oh-my/

[5] https://www.fairwarning.com/insights/wistia-salesforce-webinars/salesforce-security-evaluating-options-for-governance-and-security-monitoring-for-your-salesforce-instance

[6] https://www.metazoa.com/snapshot-use-cases-compliance-and-security-reporting/

[7] https://www.metazoa.com/snapshot-use-cases-compliance-and-security-reporting/

[8] https://www.flosum.com/release-management-best-practices/

[9] https://trailhead.salesforce.com/en/content/learn/modules/application-lifecycle-and-development-models/understand-what-application-lifecycle-management-is

[10] https://www.rackspace.com/en-in/salesforce-managed-services

[11] https://trailhead.salesforce.com/en/content/learn/modules/application-lifecycle-and-development-models/understand-what-application-lifecycle-management-is#Tdxn4tBK-heading4

[12] https://www.salesforce.com/solutions/industries/government/overview/

[13] https://trust.salesforce.com/en/trust-and-compliance-documentation/

[14] https://help.salesforce.com/servlet/servlet.FileDownload?file=015300000037bACAAY

[15] http://www.salesforce.com/in/what-is-salesforce/

[16] https://en.wikipedia.org/wiki/Salesforce.com

[17] "Secure, private and trustworthy: enterprise cloud computing with [1] Force.com", White Paper, Salesforce (Force.com)

[18] Salesforce CRM Security Audit Guide, White Paper, Salesforce

[19] Salesforce Security for the IT Executive, White Paper, Salesforce

[20] Salesforce CRM and Platform Security Overview, White Paper, Salesforce.com Confidentia.

[21] Salesforce official website, https://www.salesforce.com/, Dec. 2016.

[22] Official Salesforce tutorial, https://trailhead.salesforce.com/, Dec.2016.

[23] Salesforce documentation, https://developer.salesforce.com/, Dec.2016.

[24] The Architecture of the Apex Platform, salesforce.com's Platform for Building On-Demand Applications

[25] https://developer.salesforce.com/en/products

[26] https://developer.salesforce.com/en/Trailheads

[27] https://trailhead.salesforce.com/en/module/apex_data base

[28] Santos Asbe "On-Premise CRM to Salesforce Migration - Benefits, Challenges and Best Practices" White paper TCS.