RevCult®

How Compliance Teams Can Develop Governance Frameworks That Work

The Auditor's Guide To Salesforce

Contents:

Businesses Are Embracing Salesforce's Versatility

Commercial enterprises around the world are under constant pressure. Companies in virtually every industry have to be agile and flexible in today's hyper-paced world, and the ability to pivot on a dime — and without much notice — is what sets savvy, future-thinking business leaders ahead of the pack.

For these executives, any time is a great time to focus on improving internal processes and enhancing customer experiences. Not surprisingly, many are looking for new ways to leverage Salesforce as a tool for achieving both of these goals.

This makes perfect sense. The nearly limitless customization options that the platform offers make it extremely versatile and capable of propelling companies toward a wide variety of business objectives. Leading organizations in sectors as seemingly divergent as financial services, healthcare, CPG, and nonprofits (among others) understand this and have used Salesforce as a critical driver of value — and even as a key differentiator.

The Compliance Downside

The platform has the ability to make work more effective and efficient, and to directly impact a firm's bottom line. That's great for everyone ... almost. The reality is that everything that makes Salesforce appealing from a strategic standpoint — the customizability, the capacity to store a wide variety of data from diverse business units within an organization, the constantly evolving capabilities — makes it a tremendous challenge for compliance leaders and internal auditors.

This whitepaper will identify the challenges that compliance professionals in highly regulated industries face when it comes to Salesforce and give them a comprehensive view of what an effective Salesforce security posture looks like. Additionally, it should provide auditors with a better sense of how to establish an effective governance framework in the context of their unique business needs.

WHAT IS GOVERNANCE?

Governance is a framework to help be effective and efficient with resources to accomplish the goal of making Salesforce the system everyone wants to use.

ORG STRATEGY

- Define orgs and promotion strategy
- Set rules for changes (minor, major, hot fix, etc)
- Determine who can promote to orgs / production
- Utilize tools like source control

FRAMEWORK FOR QUALITY

CHANGE MANAGEMENT

- Select admins
- Capture requests
- Meet regularly
- Prioritize work
- Implement
- Communicate changes
- Train users on new functionality
- Support users

FRAMEWORK FOR ADDING VALUE

CENTER OF EXCELLENCE

- Educate!
- Align
- Collaborate
- Define threat models
- Innovate
- Drive road map
- Don't be scared to have more than one

FRAMEWORK FOR SUCCESS

"The right people in the right seats"

The Auditing Challenges Ahead

Compliance professionals might face any number of challenges when it comes to assessing their organizations' Salesforce orgs. In general, they're the ones who have to create an effective, repeatable process for conducting internal audits, which can be tricky if a company continually uses the platform in new ways. As the use of Salesforce across your company grows and evolves, many things happen that increase your vulnerabilities: Developers implement new code, you acquire enhanced capabilities, and users fluctuate (along with expanded permissions sets).

Moreover, many lack the appropriate tools for conducting audits. They'll often rely on little more than spreadsheets, which can result in wasted time and reporting lags as well as an increased likelihood of errors. A spreadsheet-based system also limits auditors' ability to collaborate with stakeholders, an essential part of establishing effective governance.

A lack of tools is often accompanied by a lack of talent. As the risk landscape becomes more complex and specialized, internal audit departments are struggling to find people with the skills necessary to competently assess critical risks impacting their organizations. Increasingly, leading internal audit departments must rely on third-party expertise to provide specialized capabilities to supplement in-house resources.

Salesforce Security Risk Assessment Pillars

DATA PROTECTION	How well is the data in the system being stored and protected against key threats?
DATA LOSS PREVENTION	How well is the data in the system being protected against loss?
INTEGRATION	Are integrations implemented in secure ways? Is data being accessed responsibly in the service of any integrations?
SECURITY MODEL (AUTHORIZATION)	Is the Salesforce Security Model ("Who Sees What") implemented in accordance with the organization's needs and goals?
ACCESS CONTROL (AUTHENTICATION)	Is the system accessible to the right users at the right times?
MONITORING/INSIGHTS	If data were to be maliciously accessed/used/modified, are processes and technology in place to raise awareness or support research?

A Black Box

An auditor's job is to provide verification — proof that an organization is doing what it says it's doing — in the form of evidence-based documentation. Without the tools, experience, and other resources to parse through Salesforce data and documentation, SFDC is essentially a black box (just as it is for many CISOs).

> *"Don't place complete trust in any cloud services provider. The cloud is vulnerable to cybersecurity and reliability risks."*
>
> — Steve Kennen, Proactive IT

HIPAA, the Gramm-Leach-Bliley Act on FINRA, the Sarbanes–Oxley Act, and the U.S. Securities and Exchange Commission each has a variety of regulatory drivers that auditors need to account for when validating the configuration of their orgs. Unfortunately, a lack of visibility leads many auditors and compliance teams to believe that they're more compliant than they actually are. They'll assume that once the org has been configured, the shared responsibility model shifts accountability to Salesforce.

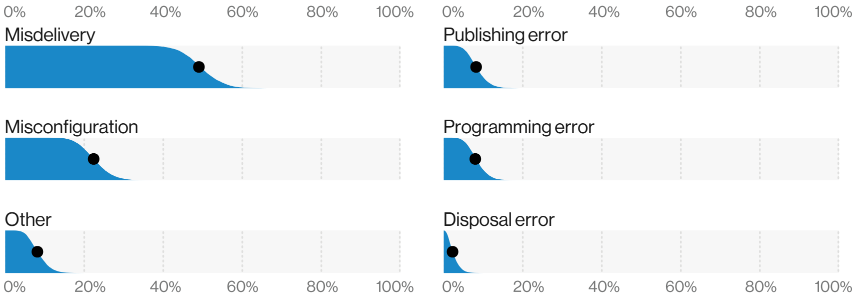
> Organizations often incorrectly assume, *"As long as Salesforce is compliant, so am I."*

This conclusion is false, but it's just one of a number of assumptions auditors might make that could ultimately lead to regulatory penalties. Another is the assumption that certain data has been classified when in fact it hasn't.

Verifying Proper Salesforce Usage

The SFDC platform is broad, which enhances its capabilities. It also includes built-in security features that make it difficult to break into, but these don't absolve users of responsibility.

Figure 67. Top Error varieties in Finance and Insurance industry breaches (n = 109)



Source: Verizon Enterprise "Data Breach Investigations Report," 2020

A few security controls are binary in terms of compliance. For SEC or GLBA filings, auditors must demonstrate that a platform has specific capabilities in order to ensure compliance. Internal auditors must ensure that the wrong people don't have access to certain information and that user profiles have the appropriate restrictions in place. However, they might not understand that their companies are using Salesforce in ways they could never have imagined. They may not have a Center of Excellence or expert system integrators managing their orgs, meaning that the audit reports they're currently receiving contain information that's inaccurate or completely false.

Too often, internal Salesforce audits — and the roles associated with them — are created as a way to check a box, not as a function for actually verifying correct usage. The reality is that it can take a long time to perform this type of assessment and that by the time the evaluation methodology has been created, even Salesforce has changed. Simply put, the reports that internal auditors receive don't always reflect that reality. Unfortunately, plenty of recent high-profile examples demonstrate this fact.

What Could Go Wrong?

In early 2019, an Amazon Web Services software engineer gained access to the account information of more than 100 million Capital One customers. The data breach was one of the largest in history and was made possible by a misconfigured web application firewall hosted by the bank in the AWS cloud. Security experts have argued about whether the bank or the cloud provider is more to blame, though the shared responsibility model that currently governs cloud contracts means that both businesses could be prosecuted.

Oftentimes, security and compliance teams within companies that use cloud platforms like AWS and SFDC assume that shared responsibility absolves them of accountability — usually when they lack the expertise or resources to establish and enforce proper governance. This mindset is most common within organizations that rush to launch cloud services (as many companies are now doing amid a scramble to set up the infrastructure required to enable remote work).

When governance, security, and compliance are sacrificed in favor of speed — and when cloud customers don't take the time to understand their security responsibilities — failure is bound to happen. In the past, organizations that failed to properly protect customer or employee data might face few repercussions. Increasingly, however, governments are enacting legislation that gives regulators teeth when it comes to prosecuting these companies.

> *"Compliance and ethics programs are at a critical juncture. They must identify regulatory and compliance risk early in digital initiatives so their organizations can rapidly respond. That requires programs to offer new services and use new and existing data sources in fundamentally different ways."*
>
> **— PricewaterhouseCoopers,** "2019 State of Compliance Study."

The European Union's General Data Protection Regulation and the California Consumer Privacy Act are just the first of what will likely be many comprehensive legal frameworks enacted to govern the use of data. The latter was cited for the first time earlier this year, in a lawsuit against online retailer Hanna Andersson and Salesforce, its e-commerce platform provider. Barnes v. Hanna Andersson, LLC was brought by a California resident and seeks to establish a class action on behalf of all other residents whose personally identifiable information might have been exposed in a breach of the retailer's network. Regardless of who wins the case, companies doing business in California will likely follow it closely to better understand their vulnerabilities under the new law.

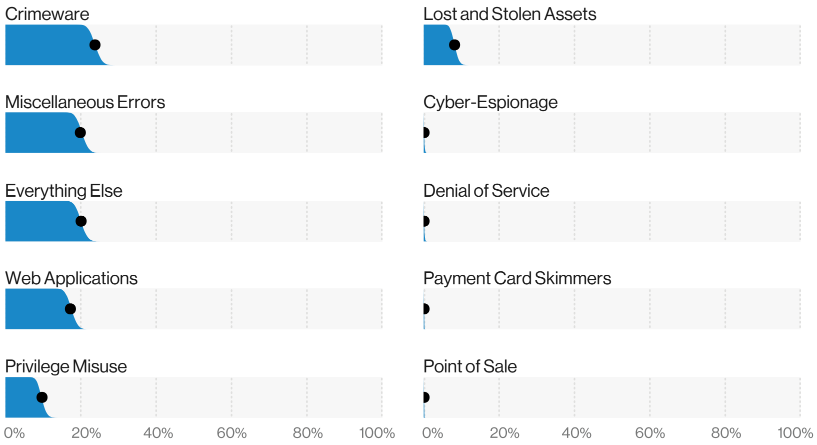


Figure 70. Patterns in Healthcare industry incidents (n = 798)

Source: Verizon Enterprise "Data Breach Investigations Report," 2020

Keeping Pace With Business Needs

The pace of business has grown increasingly fast. Asking compliance teams to match this pace is almost unfair, yet that's what they must do. Companies that have been using Salesforce since the days when it was primarily just a CRM likely have years of sprawl, and adding facilitators and implementers to that makes an auditor's job even harder.

In essence, compliance professionals are running on a hamster wheel as companies adapt their Salesforce orgs to meet business needs that might change monthly. Though this scenario may not be ideal, it's not likely to change. With that in mind, here are four tips to help compliance teams keep up:

The Right Questions and Tools

1. Ask the right questions

A comprehensive, objective data governance plan accounts for everything from compliance requirements to shareholder obligations. You can't create this plan until you know exactly what data lives inside your enterprise's Salesforce org, so that's the first question you should ask. Once you understand the nature of the information your company collects and keeps, you need to know where it's stored and who has access to it.

Vulnerabilities most often arise when the wrong people have access to the data within your platform. In extreme cases, every employee within an organization will have access to highly sensitive data, whether they know it or need it. If summer interns can see Social Security numbers, loan origination data, or bank account information, you'll need to ask why.

2. Use the right tools for the job

Excel isn't a compliance tool, and internal auditors relying on spreadsheet programs to prepare audit reports will always find themselves struggling to keep up. While Salesforce supplies different types of auditing and monitoring applications to track org usage, you'll need to find a way to efficiently document compliance.

In the time it takes to conduct a comprehensive audit and finalize it using spreadsheets, the SFDC environment can change dramatically — which brings us to our next tip.

3. Document changes as they happen

Salesforce is constantly evolving, and that alone poses a challenge to compliance teams. However, that challenge is compounded exponentially when companies continually tailor their orgs to meet a set of fluid business objectives (which could vary dramatically from one department to another).

"30% of breaches involved internal actors."

— Verizon Enterprise, "2020 Data Breach Investigations Report."

Effective Documentation and Planning

An effective governance plan is one that can account for a constantly changing environment. This includes micro-level changes — admins and developers adding new fields, new reports, new list views, etc. — as well as major pivots in the way your enterprise uses Salesforce (or any other platform) as a result of organizational or strategic changes.

4. Plan to be audited

Compliance teams should never be afraid of an audit. It provides organizations with an opportunity to assess whether a platform is really adding value and whether the existing security strategy for protecting data is sufficient.

If you're worried about an audit, it's a sign that your governance plan contains holes or that you don't have the necessary resources to effectively monitor your organization's usage. The sooner you address these concerns, the better. Failing to take this step could result in bad news when regulators do come knocking.

The Bottom Line

Salesforce is an incredible platform with almost infinite flexibility. That, combined with its ease of use, makes it an ideal tool for accomplishing a wide range of business objectives. As a cloud service provider, the company has always put an outsize focus on security, and the platform comes equipped with a multitude of both proactive and reactive security features.

Unfortunately, a platform with tremendous security capabilities can still be implemented in an insecure way. Like other features that SFDC offers, the security controls are flexible, and Salesforce isn't liable for how you configure it: That liability falls on your organization.

In some companies, developers with limited experience and expertise take governance into their own hands, without a real understanding of potential threats (external or internal) or a firm grasp of regulatory requirements. Compliance teams must often scramble to reconcile these oversights and ensure they don't happen again.

The best solution in the market? RevCult's Cloud Security Cockpit® provides a dynamic way to have real-time, high-level assessments of your security posture around customer or sensitive data at a glance, with comprehensive configuration controls at your fingertips.

Further Reading & Resources

Get a Salesforce Security Risk Assessment

Cloud Security Cockpit®: Implement, Manage, Prove Salesforce Security Controls

On-Demand Webinar: How to Make Your Salesforce Audits Auditable

The RevCult story began with a desire to help transform companies into more productive growth engines. We promoted a "revenue culture" - hence, the name RevCult - and implemented our Revenue Operating System® leveraging the Salesforce platform. Our practice has evolved as we recognize the security and data governance challenges of relying on Salesforce as a Platform-as-a-Service. While our practice has evolved, we still maintain a revenue culture, and work to provide products and services that safeguard the valuable data that our customers entrust to Salesforce. Because when your customer data isn't secure, your revenue isn't secure.

RevCult®

RevCult.com
(619) 786 - 8020