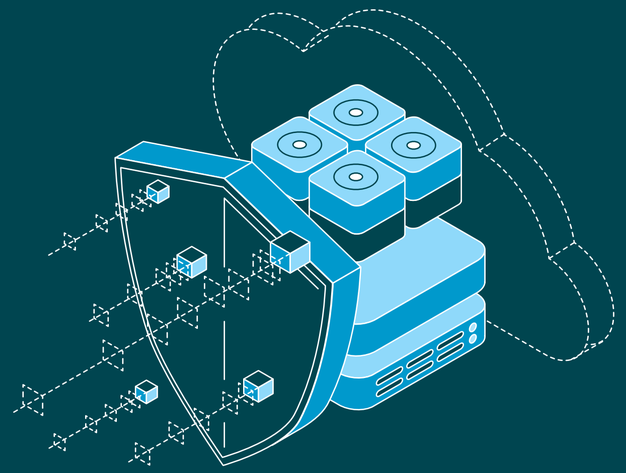
2022

Salesforce Protection Trends Report



Contents

Introduction

In the summer of 2022, an independent research firm completed their survey of **800** unbiased IT leaders regarding their involvement with protecting the data within their Salesforce deployments.

The majority **(62%)** of the Salesforce specialists were full-time dedicated to Salesforce, while most of the remainder **(37%)** also managed other SaaS platforms. Respondents were from around the world, including APJ, EMEA, and the Americas with significant tenure in their current role, including:

- **14%** with 10 or more years of experience in role
- **58%** between 5 and 10 years of experience
- **28%** less than 5 years

This was a broad-based market study on Salesforce data protection conducted on Veeam's behalf in order to understand the various personas' perspectives, responsibilities and methodologies related to protecting data within Salesforce.

This report is presented in three sections:

1.0 DRIVERS & STRATEGIES FOR PROTECTING SALESFORCE DATA

2.0 METHODS & ROLES FOR PROTECTING SALESFORCE DATA

3.0 ORGANIZATIONAL ALIGNMENT FOR USING AND MANAGING SALESFORCE

About the research

This research report summarizes the responses of three different IT roles that manage Salesforce data or the protection of it:

- **400** Salesforce administrators and consultants
- **200** IT operations generalists
- **200** backup administrators

Veeam® is the leader in backup, recovery, and data management solutions that deliver Modern Data Protection. The company provides a single platform for Cloud, Virtual, Physical, SaaS and Kubernetes environments.

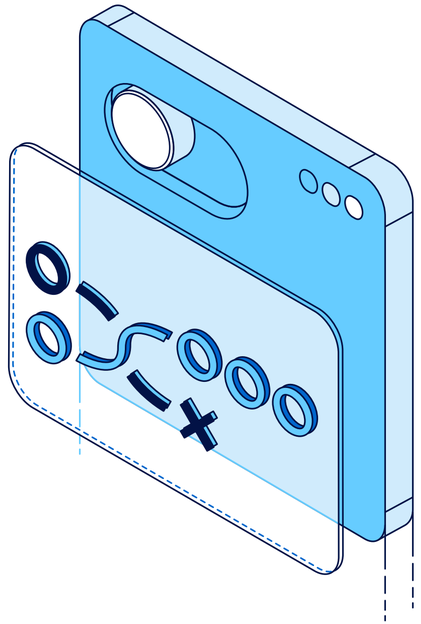
In 2022, Veeam launched **Veeam Backup *for Salesforce*.** To learn more, visit veeam.com/backup-salesforce

Questions about these research findings can be sent to StrategicResearch@veeam.com

1.0

Drivers & Strategies

for protecting Salesforce data



1.1

SaaS architecture doesn't negate the need for backup

Early in the history of Software as a Service (SaaS) platforms, many incorrectly presumed that the natively resilient architecture of SaaS negated the need for backup.

It is heartening to see that all three personas involved in Salesforce seem to equally understand that "previous versions" and "retention" are still necessary, even when the SaaS capabilities are durable. That said, it is notable and concerning that 1 in 5 **(19%)** incorrectly assume that the Salesforce platform is backing up your data.

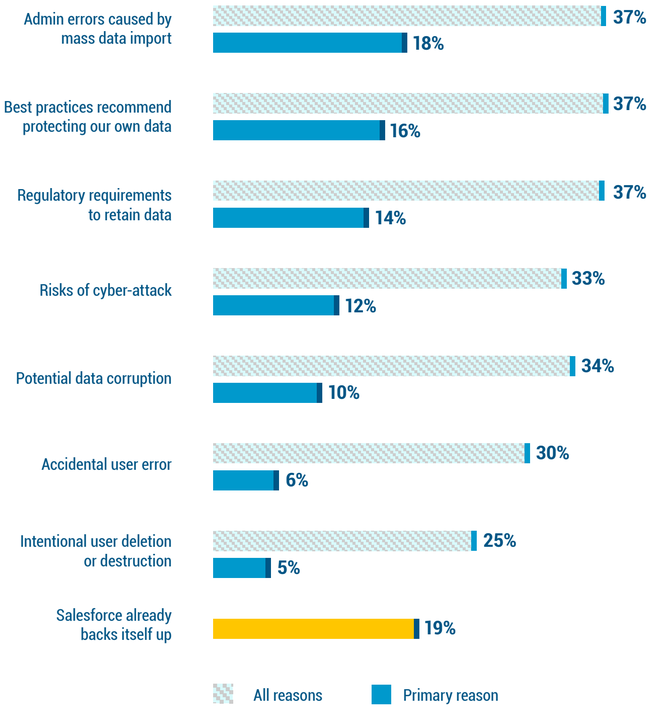
Like the database professionals before them, most IT professions acknowledge that the most important reason to protect Salesforce data is the potential for a bad import/ingest of data; while the remaining reasons are consistent with the same breadth of risks that face other IT platforms:

- Best practices & regulatory mandates
- Cyber concerns
- Errors caused by users, the application(s), or the data repositories (corruption)

This is both incorrect and dangerous to assume

Figure 1.1 Why does/would your organization protect or back up Salesforce data?

What is your primary reason?



1.2

There isn't just one reason to back up Salesforce

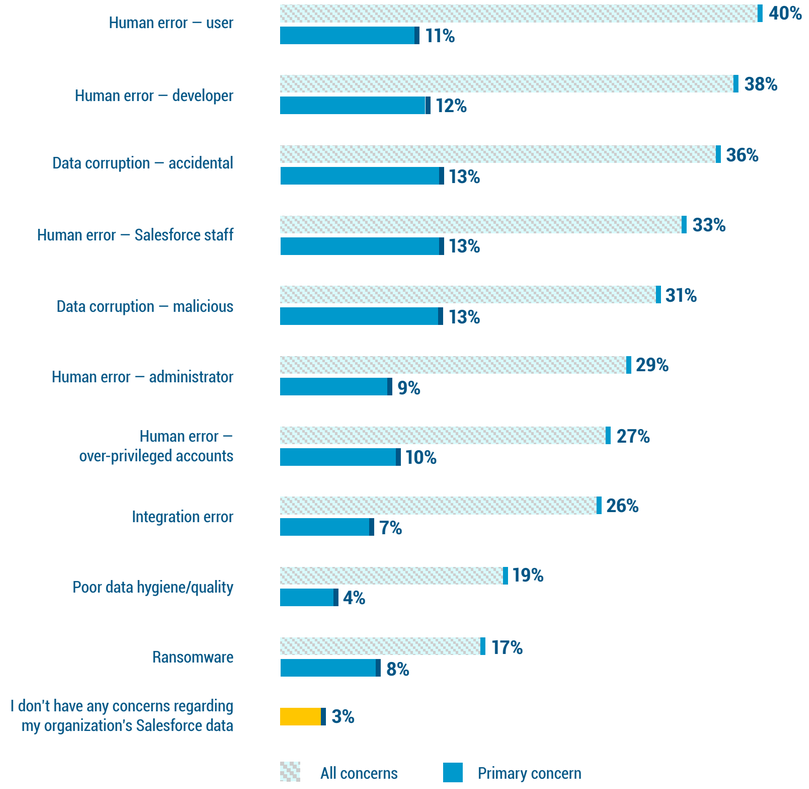
Many IT platforms have a "main reason" or prevalent concern that justifies backing up that data; and for most in 2022, that is cyber-attacks. Fortuitously, Ransomware is perceived as among the least likely concerns for Salesforce data, presumably because of the architecture — though one would presume that compromised credentials could still yield massive destruction.

That said, users and developers, as well as data corruption issues and effects from connected systems, can all impact the quality of Salesforce data and the business processes that depend on the Salesforce platform.

Perhaps the only definitive guidance is that while respondents could choose multiple concerns (only one "primary" concern), only **3%** had no concerns at all, meaning that **97%** understand the need to protect Salesforce data.

Figure 1.2 Which of the following are of significant concern to you regarding your organization's Salesforce data?

Which is your primary concern?

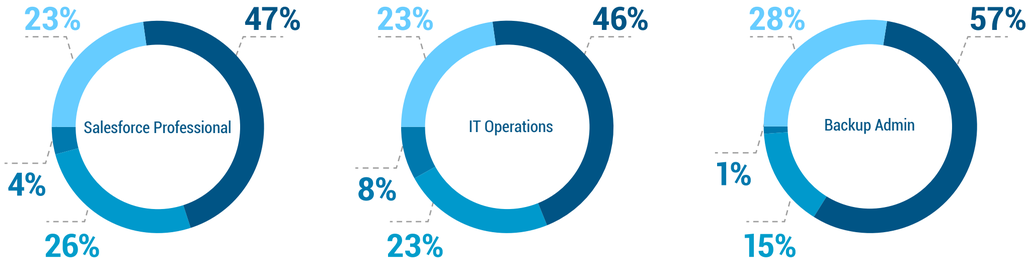


1.3

Overconfidence is dangerous

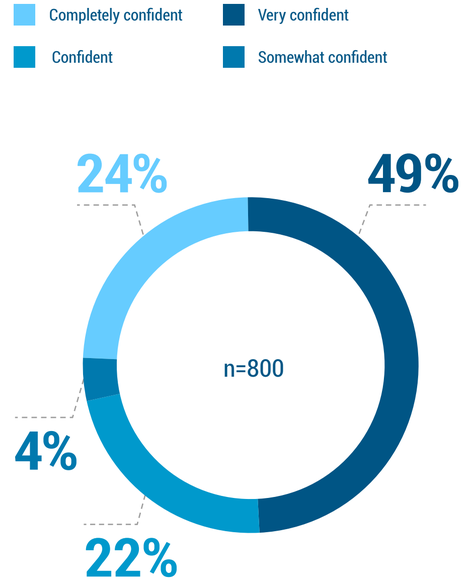
When asked about the common scenario that data integrity was affected by either a bad import or corruption, 3 in 4 organizations were either very or completely confident.

One of the key goals in this research project was to assess the alignment between the three personas most responsible for ensuring usability of Salesforce and an organization's data. When the responses are analyzed by each persona, backup administrators are notably more optimistic in their ability to restore data — arguably due to a lack of understanding the nuances and dependencies within the data constructs of Salesforce.



Noting that the Backup Admins are more confident than either SF or IT personal is particularly concerning, as it suggests that Backup Admins may not understand the nuances of recovering SF records and metadata

Figure 1.3 If there was a bad import or corruption of Salesforce data, how confident are you that you/your organization could restore the "real" data and its dependencies?



1.4

The Veeam Perspective

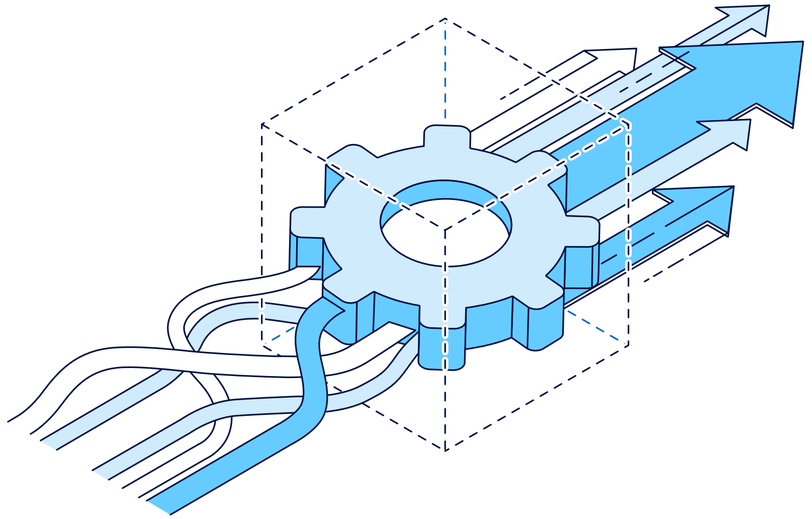
The need for a Salesforce backup, as well who is in charge of the process, has always lead to confusion within organizations. Although IT professionals agree that data loss is inevitable within an organization, they rarely back it up. Mass data imports that are common for most organizations using Salesforce are the number one reason for data corruption and deletion, and are actually handled by the professionals that are hired to keep your Salesforce data safe. Everything from overprivileged users to developers not checking code before moving to production can play a part in why organizations need to be responsible for their own data.

The Veeam approach to Salesforce backup eliminates the risk of losing your Salesforce data and metadata due to human error, integration issues, and other Salesforce data loss scenarios. Avoid data lock-in by running your backup environment on premises or in AWS, Azure and more. Download our 5-minute easy-to-read whitepaper to learn more.

2.0

Methods & Roles

for protecting Salesforce data



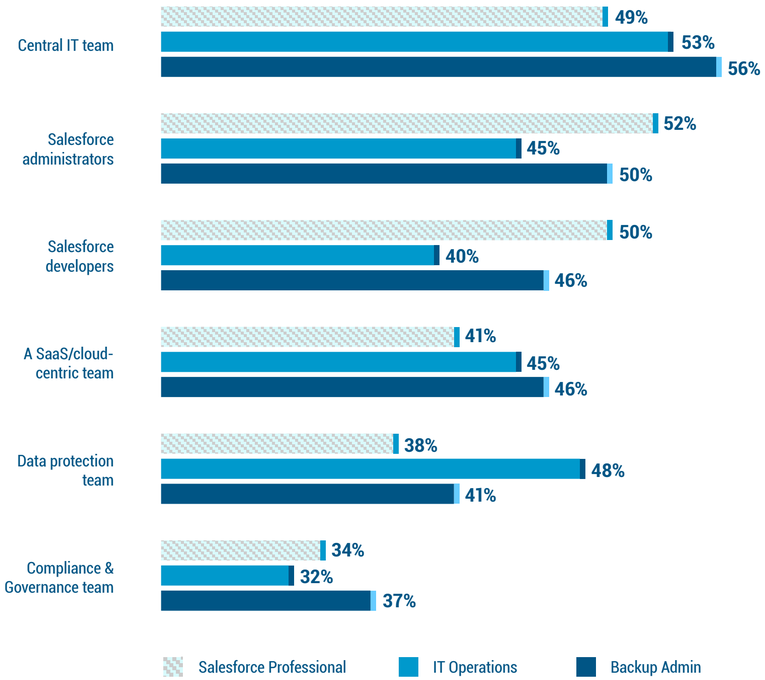
2.1

Teams are not well aligned in defining strategy

Like most IT platforms, the strategy and requirements for protecting Salesforce data seems to fall most often with the Central IT team, which makes sense in considering that the entire organization must adhere to standard operating policies and compliance mandates. Beyond central IT, most SaaS protection strategies seem to be next most affected by IT teams that truly understand that platform — e.g. Salesforce administrators/developers — a trend also seen in other SaaS discussions such as Microsoft 365.

Of potential concern is the disparity between IT Operations ("generalists") versus the relatively consistent perspectives of both Salesforce-centric and backup-centric roles — both of whom recognize the Salesforce specialists as higher (and the data protection team as lower) within determining the requirements and strategy for protecting Salesforce data.

Figure 2.1 Which team(s) within your organization are involved in determining your data protection strategy and requirements for Salesforce data?



2.2

Most agree — backups are done by backup specialists

While organizations seem to be inconsistent in how the strategies and requirements for protecting Salesforce data is, most organizations agree — with 2/3 deferring to the backup administrator and 1/3 to a Salesforce specialist.

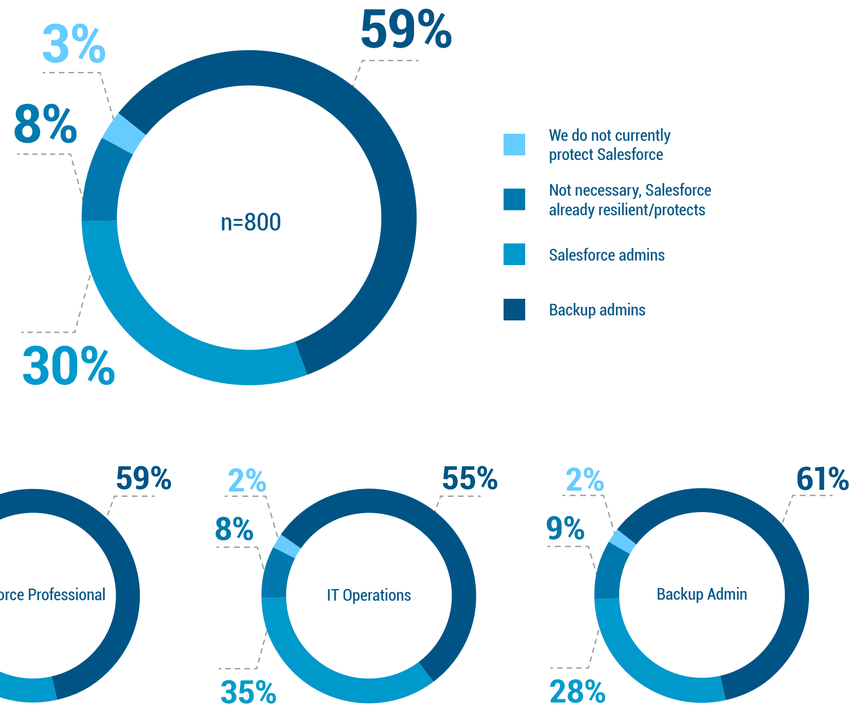
This is good news for most organizations, in that it ensures that those within the organization that are most mindful of not only operational recovery, but also BC/DR and regulatory requirements related to data retention are driving the data protection solution. This, like most SaaS protection strategies, requires close cooperation where the SaaS team must first provide credentials and perhaps support the implementation of the backup technologies; after which the same team that protects the rest of an organization's data is now protecting Salesforce data as well.

The alternative is for the backup professionals to train the Salesforce teams in regulatory requirements and then often provide the repositories (on or off site) that the Salesforce professionals send their backups to.

Thankfully, only **11%** of organizations do not back up their Salesforce data. These results are a clear indicator that the market is grasping a better understanding of the need to closely manage and protect Salesforce data.

It is alarming that **11%** do not back up their Salesforce data

Figure 2.2 In general, who manages the protection of Salesforce data overall in your organization today?



2.3

Most aren't retaining their data long enough

Organizations face retention (or deletion) mandates across their IT spectrum, regardless of which technologies or platforms they choose to use. That means that regardless of on-premises servers, cloud-hosted machines, or SaaS applications, retention mandates still generally apply (by data type or contents).

As such, it is not surprising that most organizations reported **(Figure 2.3)** having retention mandates starting at 3 years, most being greater than 5 years, but many requiring 20 years or more.

What is surprising is how few organizations reported **(Figure 2.4)** actually retaining their Salesforce data for even six months, much less what might adhere to modern regulatory or operational best practices. **This is reminiscent of traditional database administrators who would only keep data long enough for rollbacks, without regard to retention mandates for all corporate data.**

Figure 2.3 What data retention mandates need to be applied to data for Salesforce data in your organization?

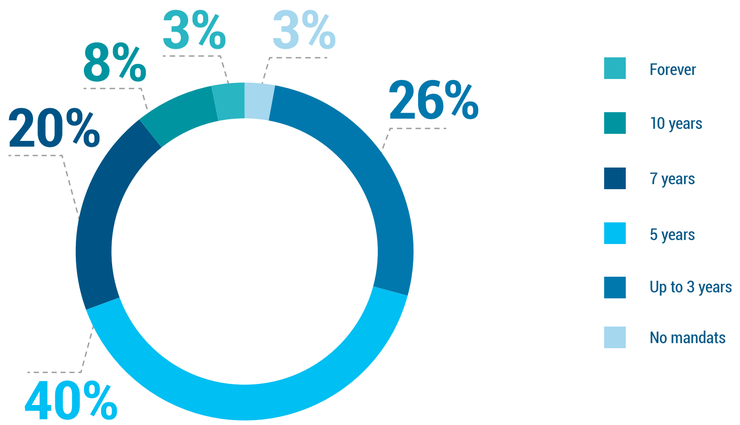
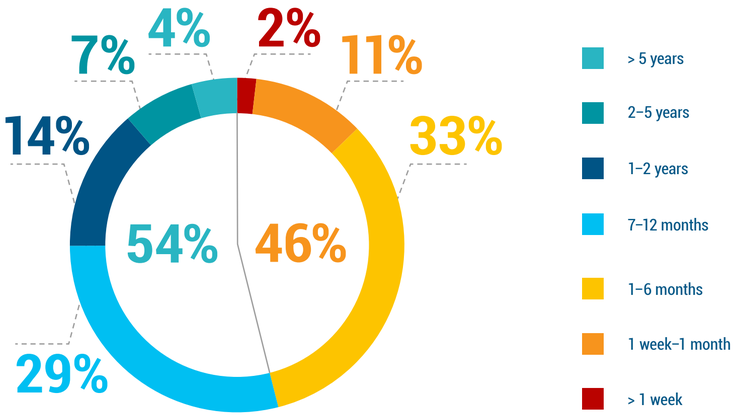


Figure 2.4 How long does your organization retain, or plan to retain, copies/backups of data from Salesforce?



It is unexplainable why there is such a break between how long they "must" and how long they the "do" retain data

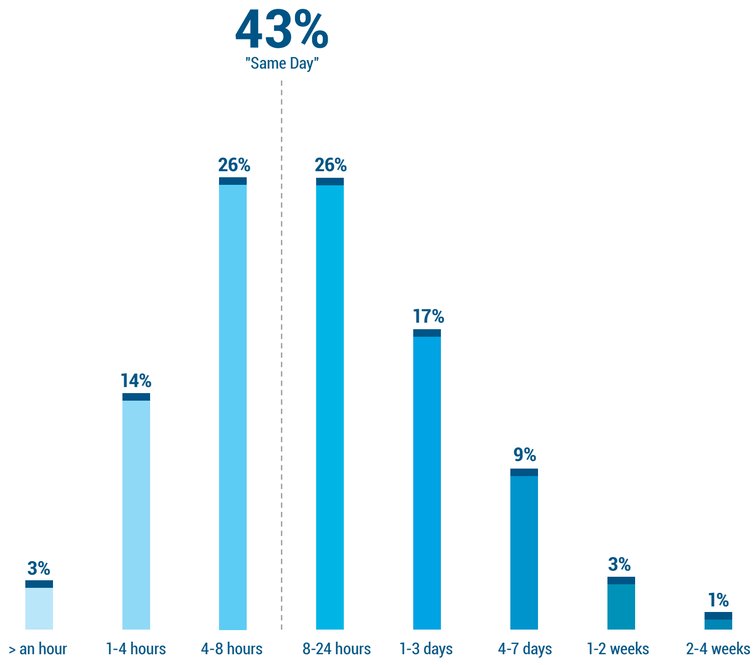
2.4

Even "simple" problems take longer than you think

While most IT backup discussions revolve around overwritten or deleted discrete objects (files, mail messages, etc.), Salesforce data is mostly centralized not just around individual records, but their respective accounts and the metadata and dependencies of those records.

Thus, organizations should be concerned when discovering that less than half **(43%)** of organizations could restore even **100** accounts (and their records and associated dependencies) within the same business day (up to eight hours). Just as alarming, **30%** of organizations would require multiple days or weeks for such a restoration.

Figure 2.5 Imagine that you have somehow lost 100 accounts and their related records. Approximately, how long would it take you/your organization to restore your Salesforce data, including metadata and its dependencies?



2.5

The Veeam Perspective

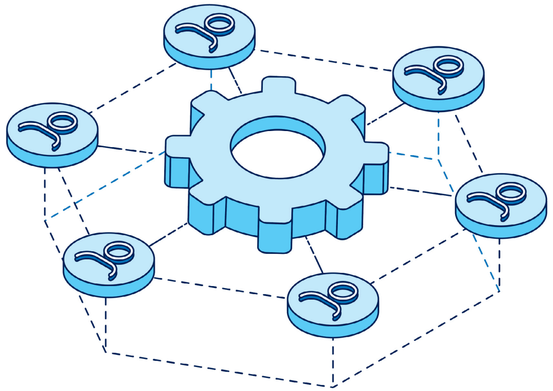
One of the biggest issues organizations tend to deal with when data is missing and needs to be retrieved, is who exactly is responsible for creating a data protection strategy and Salesforce requirements within the organization. It could be IT, the Salesforce Admin, or the Salesforce Consultant. Trying to backtrack and figure out who should have a backup plan in place usually happens after a data loss with no chance of recovery. Salesforce data retention is also often not top of mind, as most organizations claim to retain their Salesforce data for less than a year. This short period of time often does not fulfill retention mandates, as well as losing large amounts of contacts could be devastating to a sales team. With so many people touching Salesforce, it can be hard to know what changes are being made, and how long it might take to discover those changes. With less than half of organizations feeling they could restore data and metadata within 24 hours, where would that leave your team with no access to their data?

Veeam Backup *for Salesforce* eliminates the risk of losing your data due to human error, integration issues, or other Salesforce data losses. With incremental sync and flexible scheduling, you can back up your Salesforce data almost continuously. Set your backup to hourly and remove the fear of data loss.

3.0

Organizational Alignment

for using and managing Salesforce



3.1

Most organizations run multiple production Salesforce instances

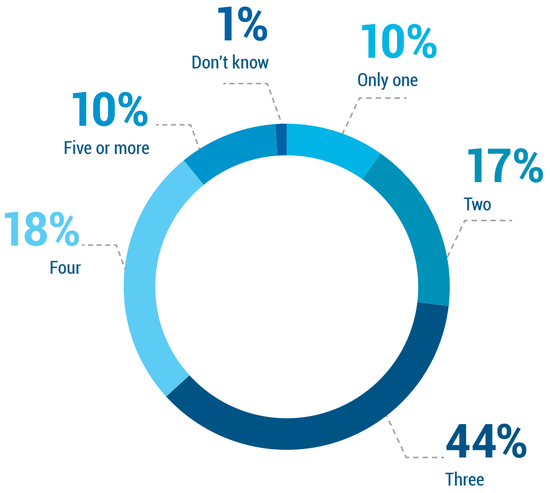
With apologies for the imprecise nomenclature, most organizations (companies/institutions) run multiple Salesforce “organizations” (implementations/data-sets), often due to separate operating entities, business functions, or simply geo/functional boundaries.

Only **10%** of respondents stated that they only operate one production “organization” or instance of Salesforce. That said, when those respondents were asked how those multiple instances were administered, most were managed centrally:

- **41%** had all centrally managed
- **51%** had most centrally managed
- **7%** had some centrally managed
- **1%** made each have its own administrator

This is good news when considering that backup admins are most likely to be conducting the backups themselves; thus, easier to ensure collaboration and comprehensive protection across the myriad Salesforce implementations.

Figure 3.1 How many production "Salesforce organizations," not including Dev/Staging or Sandboxes, does your company operate?



3.2

Aligning with “the rest” of IT

In considering that the strategy for protecting Salesforce data **(Figure 2.1)** is often driven by Central IT, while the backups themselves are most often conducted by the team that does backups across IT **(Figure 2.2)**, respondents were asked how aligned is the Salesforce team with both Traditional IT and the other SaaS teams.

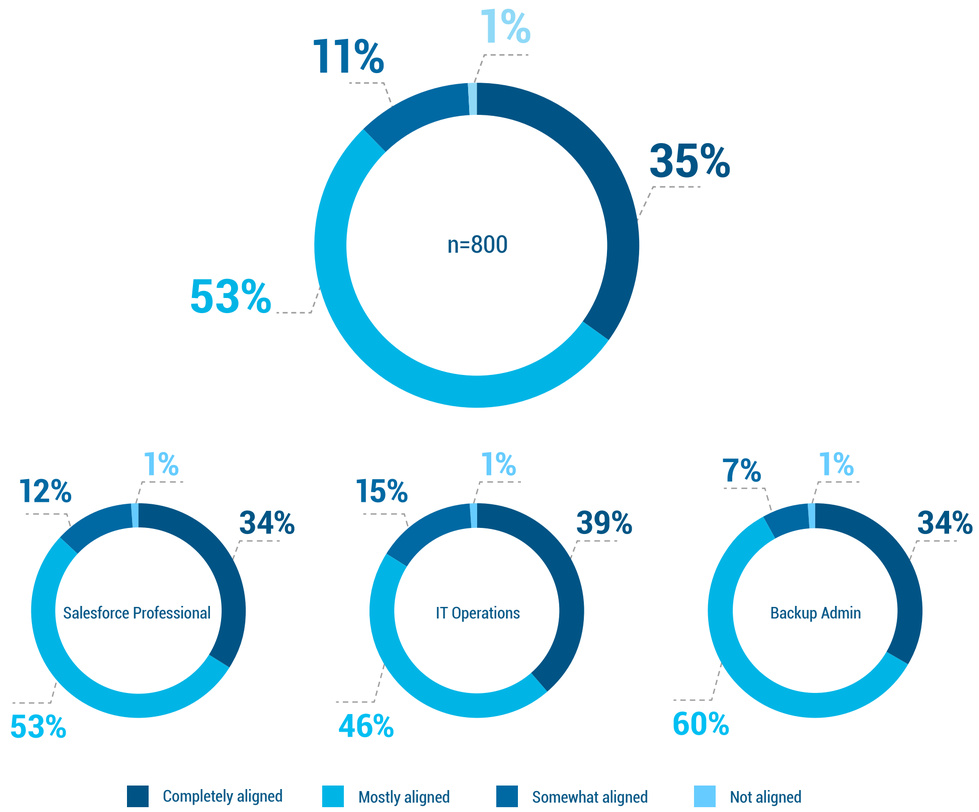
While **Figure 3.2** reveals that the majority consider the teams completely or mostly aligned, a closer look by persona does show that the Backup team (which is typically part of traditional IT) believes a higher level of alignment than the other personas.

When respondents were asked how aligned the Salesforce team was with other SaaS (e.g. M365) teams, a nearly identical result was found:

- **36%** said completely aligned
- **54%** said mostly aligned
- **9%** said somewhat aligned
- **1%** said not aligned

This bodes well for ensuring continued improvement as organizations align the protection of Salesforce with the protection of the rest of their IT environments.

Figure 3.2 In terms of team and strategy in your organization, how aligned is the Salesforce Team with the “traditional” IT teams that manage data center server platforms?



3.3

The Veeam Perspective

It is good news to see that over 80% of organizations feel their Salesforce and IT teams are in alignment. Veeam feels it is important for teams to understand the importance of data protection across all platforms within an organization, so the persona roles that are responsible for the other pieces of their IT environment also see the need to back up their Salesforce environments.

Some important reasons to align your Salesforce team to other SaaS teams include having a clearer strategy when suggesting behaviors and solutions that can be applied across multiple environments, as well as the ability to set standards and benchmarks to be cohesive. Sharing data backup and recovery plans across environments and teams can help with establishing your recovery goals, as well as determining the best strategy to retain your Salesforce data and metadata.

Veeam Backup *for Salesforce* is powered by Salesforce APIs, and allows you to deploy on premises or in the cloud. To learn more, visit www.veeam.com/backup-salesforce.html

Summary

This analysis covers Veeam's first broad-based market study on the management and protection of data within Salesforce. Based on the findings from these results from **800** IT professionals who are either Salesforce specialists, Backup admins or IT Operations:

- There is broad recognition of a diverse range of reasons to protect Salesforce data, including users, developers and admins making errors, as well as technically caused errors from corruption, integration and bad imports.
- Most agree that Central IT is most often defining strategy for all workloads, including Salesforce, with frequent input by Salesforce specialists — but the backups themselves are most often conducted by the backup administrators OR under their oversight by the Salesforce specialists.
- Too many organizations may be overly confident in their ability to restore data after experiencing data corruption or a bad import, particularly for those less aware of the metadata dependencies within the Salesforce applications' framework. That said, the underlying message is that respondents see the importance in recoverability when it comes to their Salesforce data.

Organizations recognize the need for longer-term retention of data that aligns with overall operating and regulatory requirements, but most Salesforce data retention implementations currently fall short of those mandates.

The philosophies for protecting Salesforce data are surprisingly manager when compared with similar research on other SaaS platforms (e.g. Microsoft 365), even though the tools available to achieve the protection of Salesforce data are less available; particularly when endeavoring to protect Salesforce holistically by mature heterogeneous enterprise backup offerings.

For questions on this research or its usage: StrategicResearch@veeam.com

Click to download additional materials from this research

About the authors

Jason Buffington
VP, Market Strategy

@JBuff

@jasonbuffington

Dave Russell
VP, Enterprise Strategy

@BackupDave

@backupdave

Julie Webb

Director,
Market Research & Analysis

veeam.com