FINICAST

schellman
Quality, above all.

Managing the Exposure of Confidential Data when Collaborating with Spreadsheets

Managing the risks of executing operational processes across the company while collaborating on spreadsheets that contain confidential information.

Authors:
Marco Santiago (Finicast) and Rebekah Skeete (Schellman)

Spreadsheets are often a critical element of business workflows. Unfortunately, individuals often turn a blind eye to the risks of sending spreadsheets with confidential information across vulnerable channels. Every organization needs to carefully consider what security, privacy, or operational risks it takes on when it continues to use office applications and user messaging tools as its primary means of collaboration and data exchange.

Collaboration with spreadsheets for business workflows needs to be reimagined with better tools.

Lack of Security Means Exposure for Finance and Operations Data

Most modern security and privacy programs start with a wise two-step process:
1. Classify data and assets into appropriate security classes
2. Determine what security provisions are needed for those security classes

For many organizations, the focus falls on the information assets classified as core to production, i.e., information from clients or customers, information that facilitates their primary operations, regulated data (e.g., ePHI), or the like.

As a result, other confidential information often gets overlooked. There could be broad classifications for confidentiality like information from finance, HR, or operations, but rarely does an organization's security program or awareness extend to the everyday occurrences of how they manage these data.

In truth, finance teams and business operations groups handle sensitive or confidential information all the time, and, frequently, they do so with little direction from security or compliance, with almost no training that speaks to their situation, and with few controls for oversight.

Why do companies continue to overlook security when sharing data? **Collaboration.**

Security often receives little attention or priority while using common collaboration tools such as spreadsheets and emails. Most organizations use both. Even with the appropriate policies in place, few groups or employees understand how to consider their use in everyday work and these applications lack the proper controls, creating both security risks and operational headaches:

Emails containing sensitive financials may be sent to the wrong recipient or—if they are sent to a legitimate recipient—they reside in a local or cloud storage space which may not have appropriate controls

Spreadsheets are often difficult to partially redact when necessary
The reported issue of a staffing spreadsheet where someone merely hid the column containing sensitive compensation data rather than removing it has occurred so many times that it has passed into legend.

While that issue is embarrassing and problematic, the idea that sensitive information may leak prematurely beyond the confines of the organization has possibly more dire implications for the company's health at large, particularly for publicly traded companies or those looking to woo investors.

When managing spreadsheets of company data, an aspect of security that often goes overlooked is that of privacy. Regarding data sets containing customer or employee PII — even seemingly innocuous elements like email or IP addresses can qualify as PII in certain circumstances — or similarly regulated data, organizations may have privacy obligations. Organizations may need to track where that data resides and how long they are kept, while also ensuring they delete any such data when no longer needed or after responding to data subject requests (e.g., right to be forgotten requests).

Organizations with clear sets of structured data, handling these requirements comes down to a matter of good procedure. But for those who use numerous iterations of spreadsheets distributed across various user inboxes, Slack channels, or similarly unstructured file space, the idea of finding all instances of a user record to delete to comply with a data subject request under GDPR or HIPAA quickly turns into a mind-boggling nightmare.

Aside from said security or privacy concerns, relying on unstructured data sources and messaging applications can easily create operational difficulties:

- Wide distribution of stand-alone sheets over email can lead to problems maintaining revision history
- Distributing the correct document
- Incorporating multiple updates at once

Modern office applications — such as Office 365 or Google Docs —partially solve the multi-user and distribution problems. Unfortunately, more sophisticated tasks involving more granular access control remain beyond the ability of these existing tools. There type of more sophisticated challenges include:

- Ability to track who made what change when
- Ability for someone to review and approve a colleague's work before incorporating it into the larger work
- Ability to reject or delete information with corresponding audit trail

Spreadsheets. Are their security limitations your achilles heel?

Spreadsheets are often a critical element of business workflows such as planning, forecasting, and reporting. Since these workflows tend to be time-sensitive and require collaboration from stakeholders across the company, individuals often turn a blind eye to the risks of sending spreadsheets with confidential information across vulnerable channels to execute tasks in a timely manner.

Of course, it is possible that, when sharing traditional spreadsheets, users may leverage the available security features such as password encryption on workbooks, protecting worksheets, and hiding columns or rows. But since the goals of these features are to prevent unauthorized access to data and limit data or functionality relevant to business workflows, they also limit the ability to collaborate and actually complete the required tasks to deliver on the goal of the workflow.

These features are flawed, despite being the only tools available in traditional spreadsheets today for the following reasons:

- Analysts and business users need to share and collaborate on spreadsheets to make company data more useful
- Excel and Google Sheets are the most common and most accessible tool to share, analyze, and report financial or operational data
- Email and messaging apps are the utilized heavily for collaboration in any organization

These spreadsheet challenges occur at nearly every business. Every organization needs to carefully consider what security, privacy, or operational risks it takes on when it continues to use office applications and user messaging tools as its primary means of collaboration and data exchange for its finances, accounting, or similar operational functions.

Business users deserve and need a better solution. Reimagining Spreadsheet Collaboration

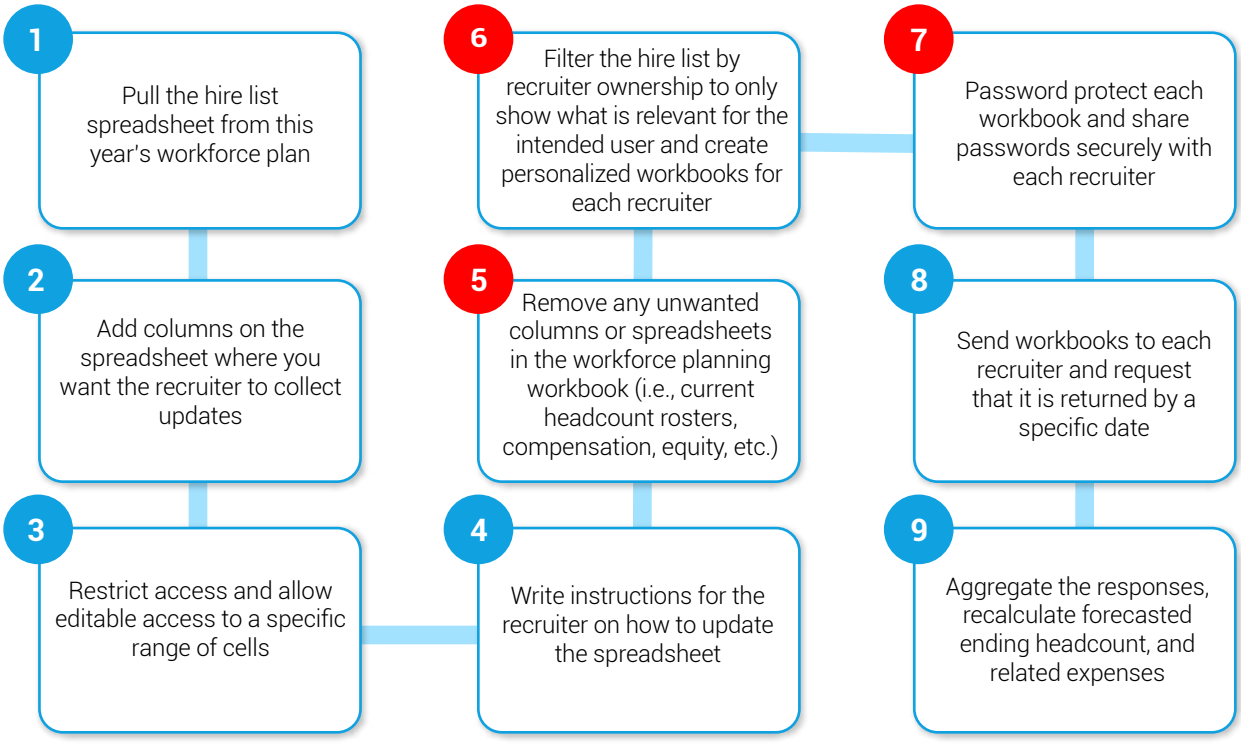
Finicast is a collaborative planning platform like Excel and Google Sheets. However, Finicast offers substantially more power for activities such as multi-dimensional data analytics, as well as security features required for meaningful collaboration involving sensitive information. Unlike existing applications available in the industry, Finicast provides security and privacy capabilities in the following areas:

- Authorization: Users authenticate their identity before logging into the application
- Permissions: Allowable actions for a user within the application
- Tracking: Ability to track all changes made by any user
- Collaboration: Multiple users can work on multiple versions of a model simultaneously and support structured review and approval according to the nature of a change

Example: Financial Planning & Analysis

Let's take a look at a business workflow that requires confidential data for workforce planning to fly around the company in spreadsheets. For example, a Financial Planning & Analysis (FP&A) team requests inputs from a recruiter on the open job positions planned for the upcoming year to provide the CFO with an updated headcount forecast.

Traditional Spreadsheets Approach:



Imagine someone on the FP&A team forgot any step between 5 through 7. Confidential data would then be compromised, and unfortunately, very little can be done once that information is exposed via a shared email or sent message containing a traditional spreadsheet.

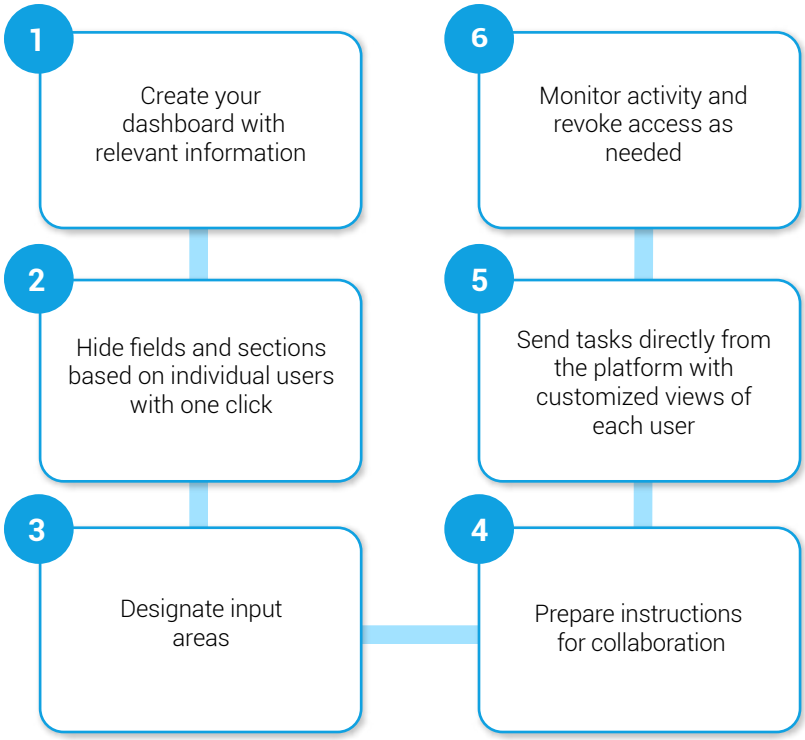
The process is simply difficult to manage and painful due to the following:

- Managing the quantity of spreadsheet become unwieldy among so many business stakeholders
- Preparing files becomes extremely time consuming
- Reviewing spreadsheets builds 'review fatigue' and things are simply missed
- Propagating errors persist and multiply unless all individual spreadsheets are reviewed and corrected
- Tracking which passwords have been shared and used by whom is impossible

A New Approach: Bidirectional Dashboards

What if the FP&A team could build real-time bidirectional dashboards that enable collaboration throughout the enterprise? Rather than traditional spreadsheets, this would allow for the collecting and sharing of sensitive information without compromising data confidentiality requirements, and still provide the context to complete all the business tasks in a timely manner.

Here is a new flow:



- **Create your dashboard with relevant information**
  With any business workflow, you need to provide a business users with relevant information so that they can provide thoughtful feedback. The problem is that dashboards usually provide information one way and spreadsheets are mechanisms to collect that feedback. Dashboards should be a bi-directional experience where business users can consume as well as provide inputs back in real-time.

- **Hide fields and sections based on individual users with a few clicks**
  Access to spreadsheets is usually customized for the individual viewing the data. Business users need to hide certain fields and define access based on a rule of who is viewing it.

- **Designate input areas**
  Access to spreadsheets is usually customized for the individual viewing the data. Business users need to hide certain fields and define access based on a rule of who is viewing it.

- **Prepare instructions for collaboration**
  Instructions need to be written clearly and additional context should be provided on the dashboard for proper collaboration.

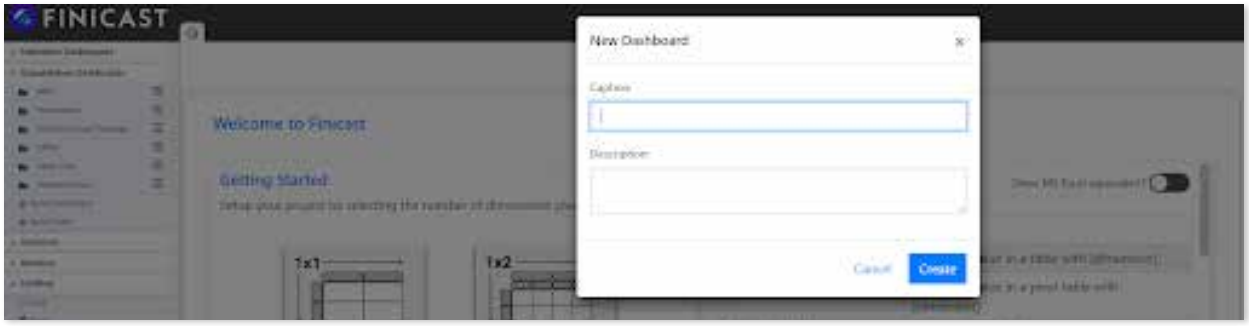
- **Send tasks directly from the platform with customized views for each user**
  Business users will send out a task through the application using the prepared dashboard that is filtered for the proper authorization and permissions. The task is emailed with a hyperlink to the individualized dashboard. The security of each link should be controlled by an application.

- **Monitor activity and revoke access as needed**
  Business users manage the task based on the completion of each user. Monitor if the emails have been opened and send reminder emails. Verify what users can see and review the activity logs of each user.

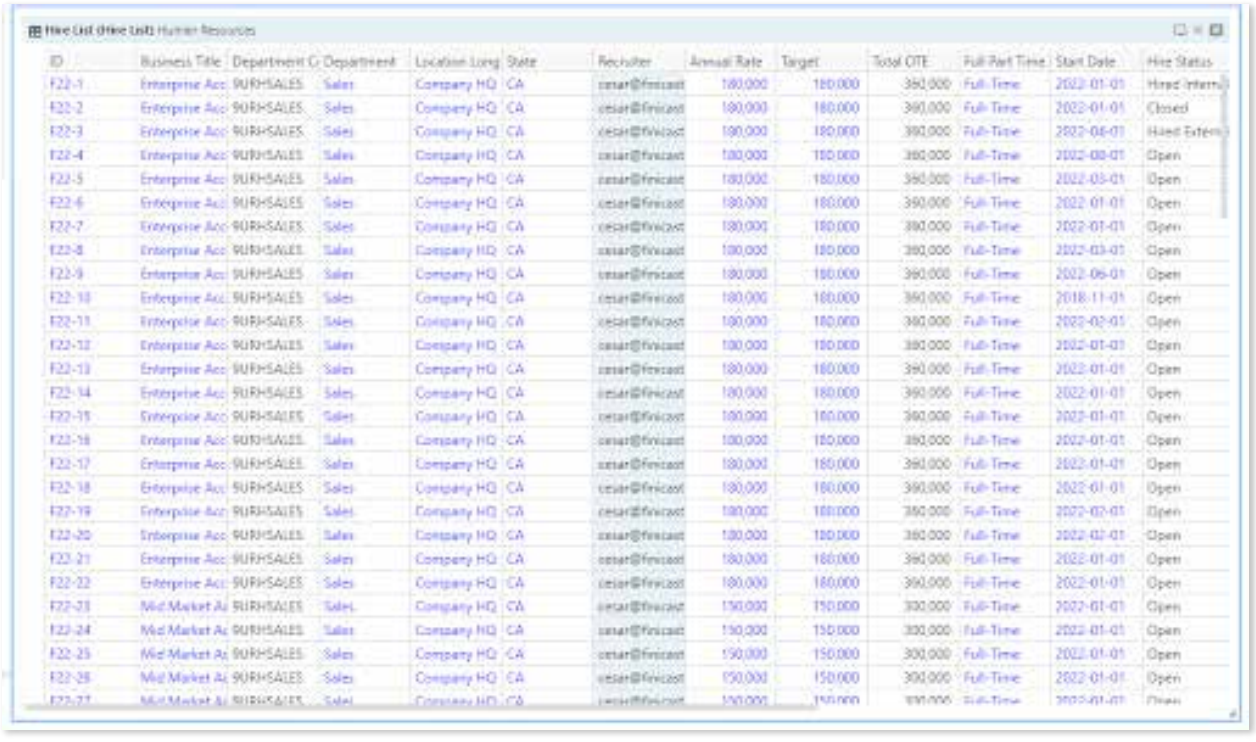
Bringing it to Life with Finicast

Create your dashboard with relevant information

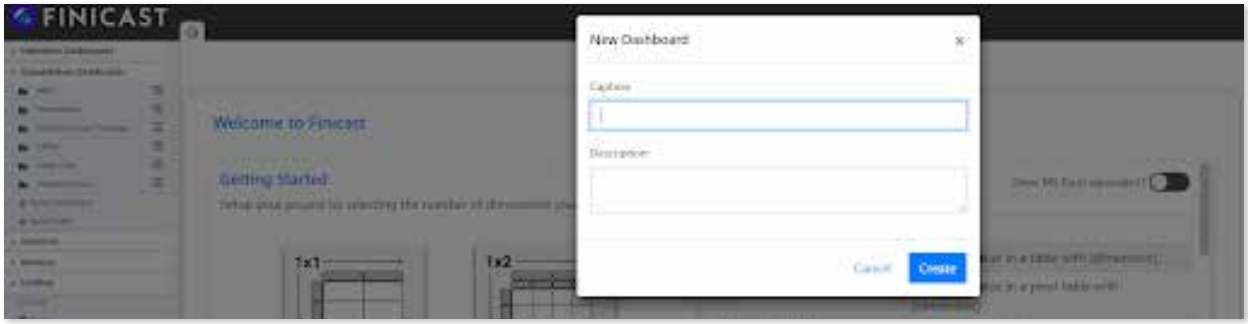
When creating a dashboard, add all the tables you want on a dashboard for the end user to view and provide additional relevant data for the recruiter.



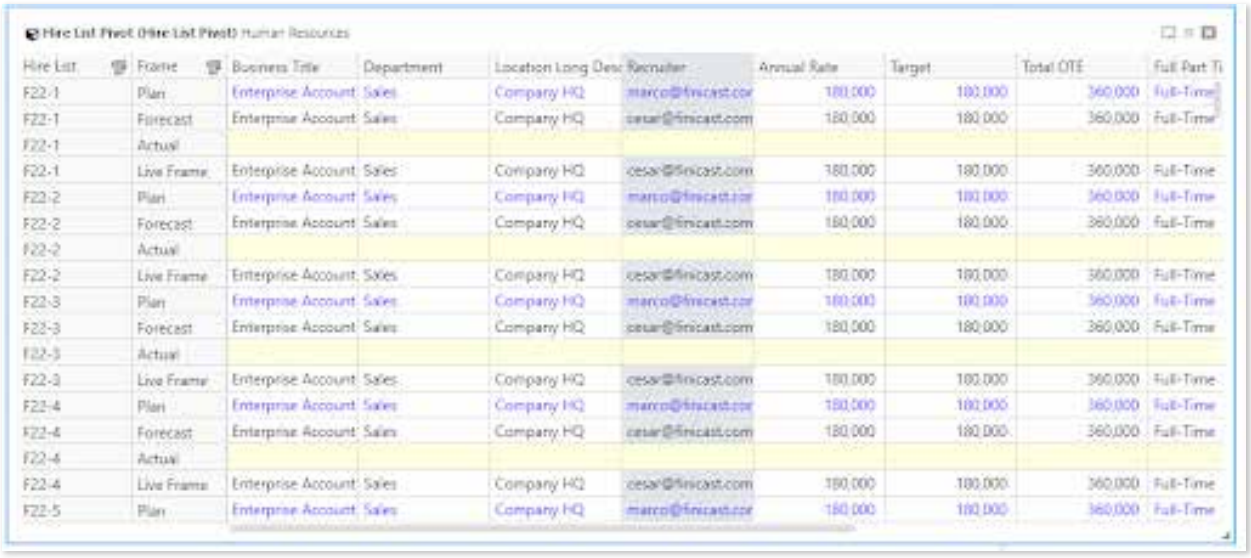
Add the latest hire list to the dashboard.



Include a pivot table of the hire list that tracks Plan, Forecast, and Actual:



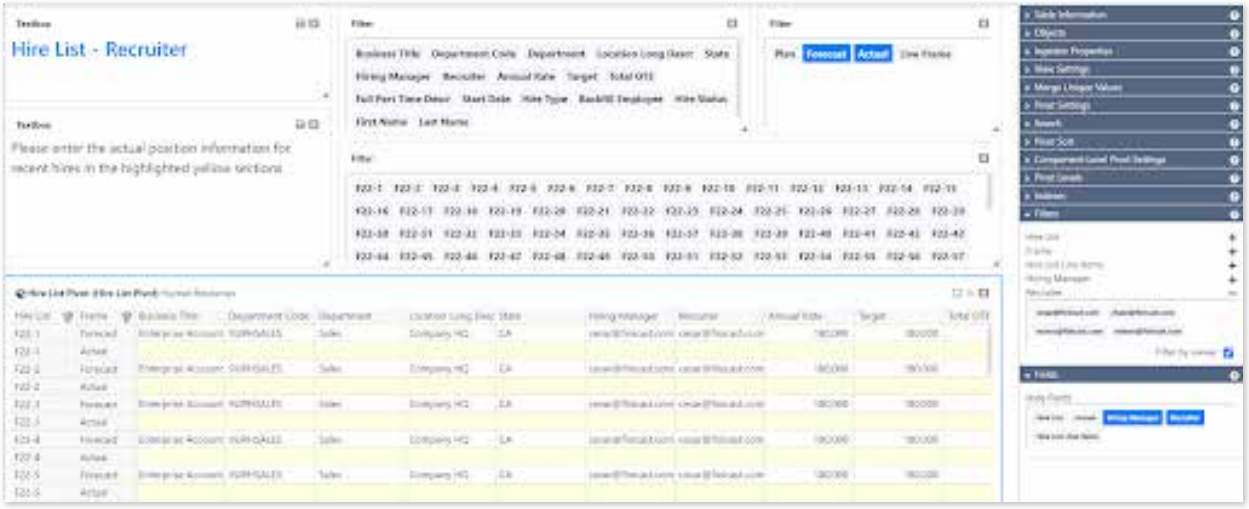
Notice that a recruiter email is associated with each line item in the above tables—that is to ensure proper authorization for each recruiter.



Hide fields and sections based on individual users with a few clicks

Finicast also allows you to:

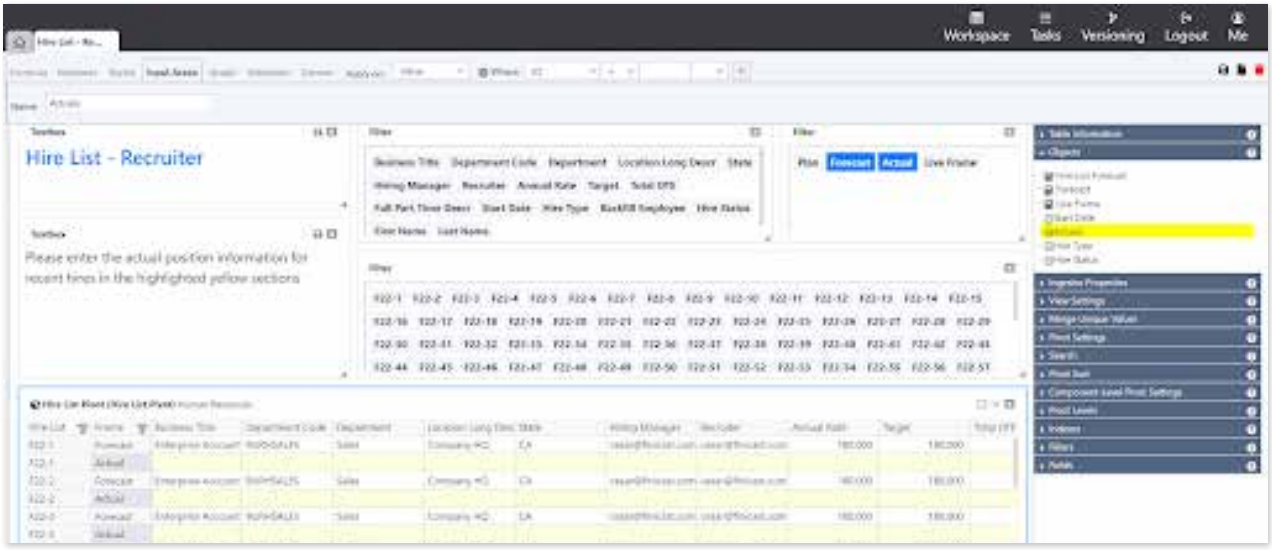
- Customize views by hiding unnecessary fields (Hide Fields section - highlighted blue);
- Filter the pivot table for what is relevant to the user (Filter selection - highlighted blue); and
- Customize the view access based on the user email (Checked - “Filter by viewer”).



With all these security features, users can only see the records that have been assigned to them (“Recruiter”). When each recruiter opens this dashboard, they will only see a user-specific dashboard. As a result, business users no longer need to create multiple spreadsheets and slim down confidential data for authorized access.

Designate input areas

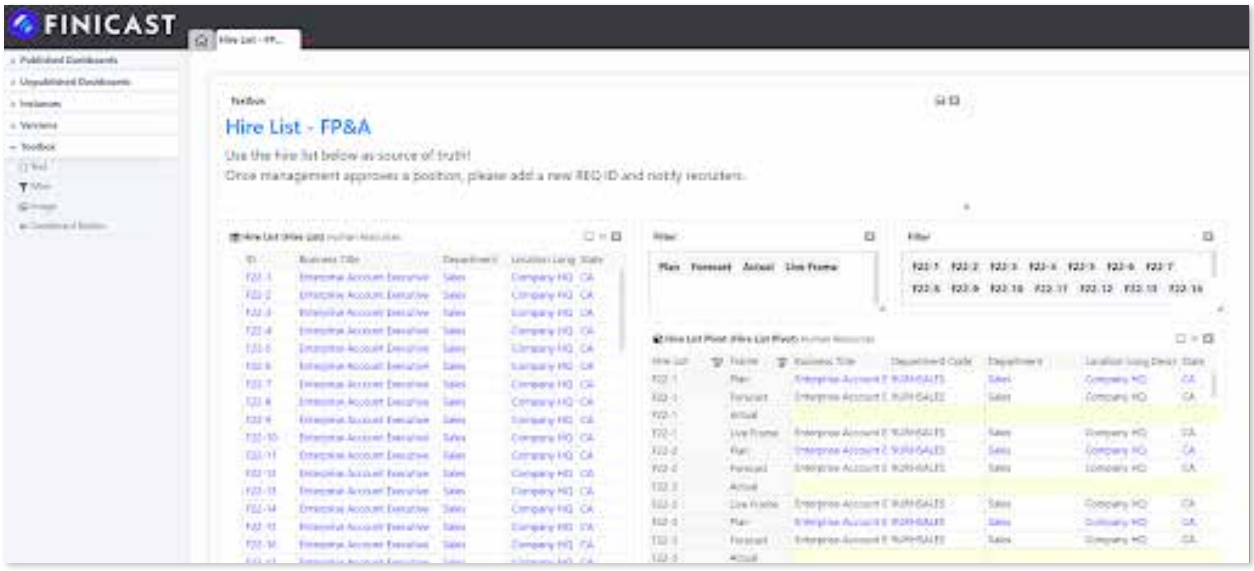
Eliminate the fear of someone compromising the spreadsheet by designating specific cells that can change. Set input areas (highlighted in yellow) for users so that stakeholders can make changes only on the cells that need input.

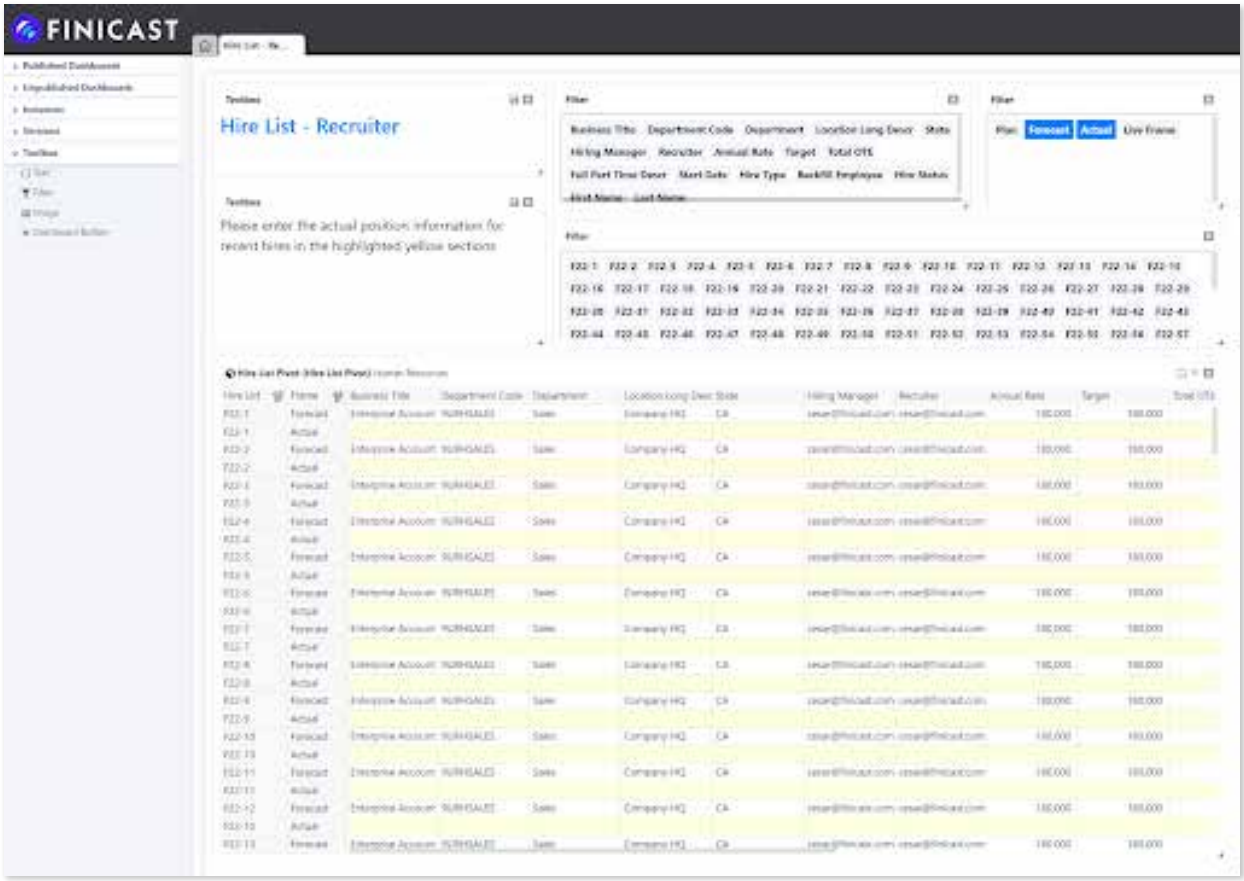


Prepare instructions for collaboration

Use a text box to add instructions and explanations on how to use the dashboard.

Below is the Finicast bidirectional dashboard created for the aforementioned workforce planning scenario to be shared with the FP&A and recruiting teams.

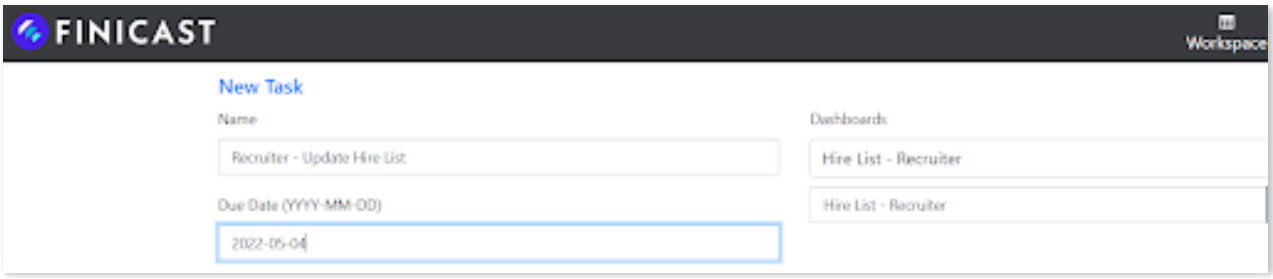



FINICAST
Hire List - Recruiter
Please enter the actual position information for recent hires in the highlighted yellow sections

Send tasks directly from the platform with customized views for each user

Finicast also features a robust task management system that sends these bidirectional dashboards as a task and tracks the workflow with the related data.
In this example, tasks and data are shared for forecasting headcount.

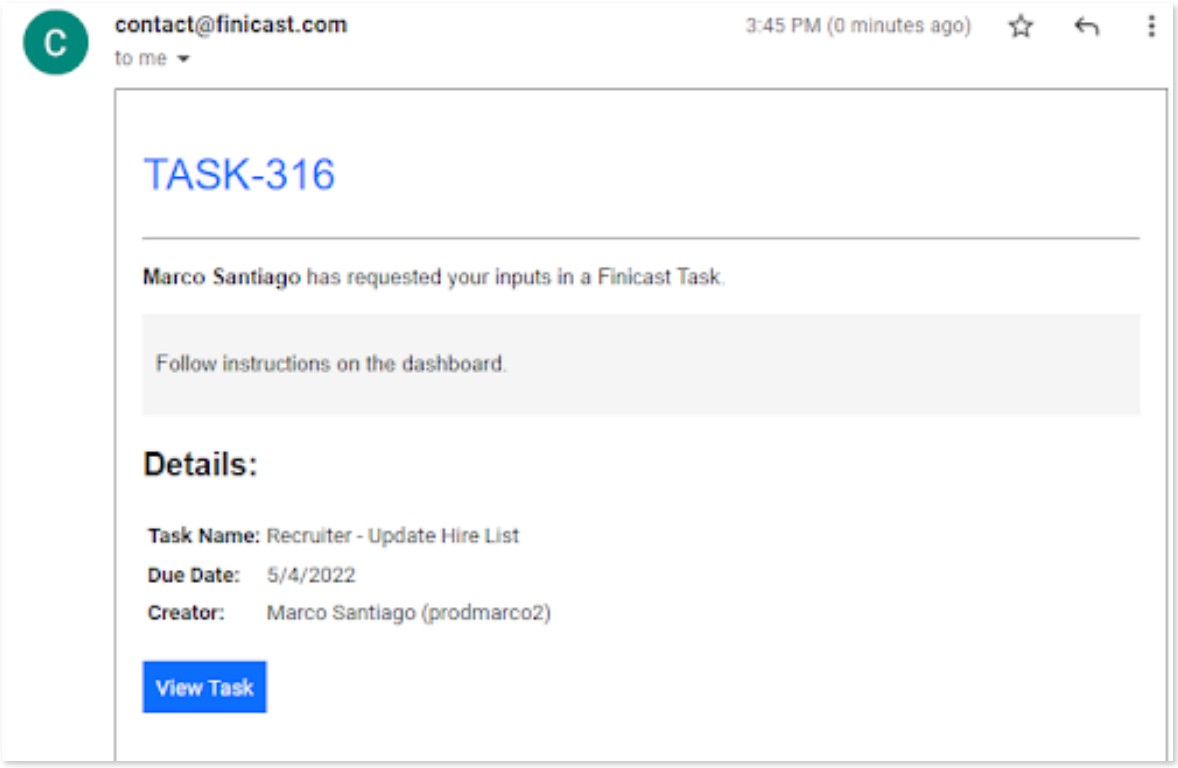
Create a Task and Attach the Dashboards to Send Out



Require Login within a Finicast Account For Dashboard Access

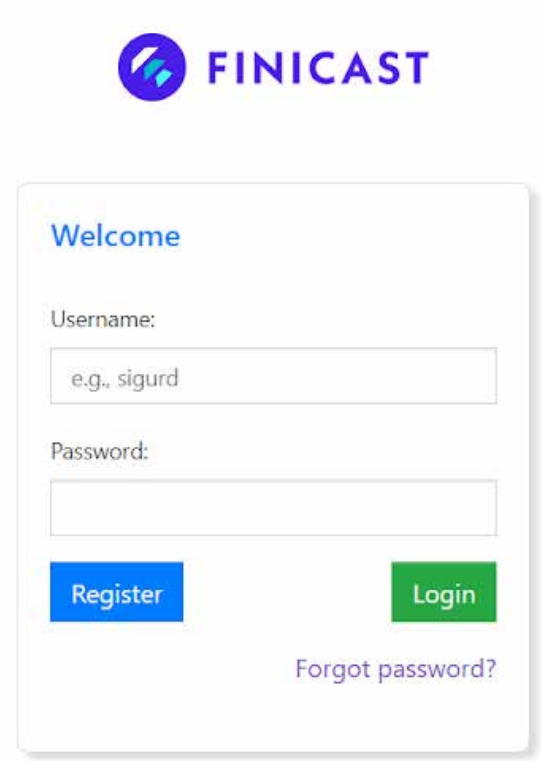
Email the Bidirectional Dashboard and Task Users Identified in Your Tables Access

Require Login to See Tasks and Ensure Authorized Access

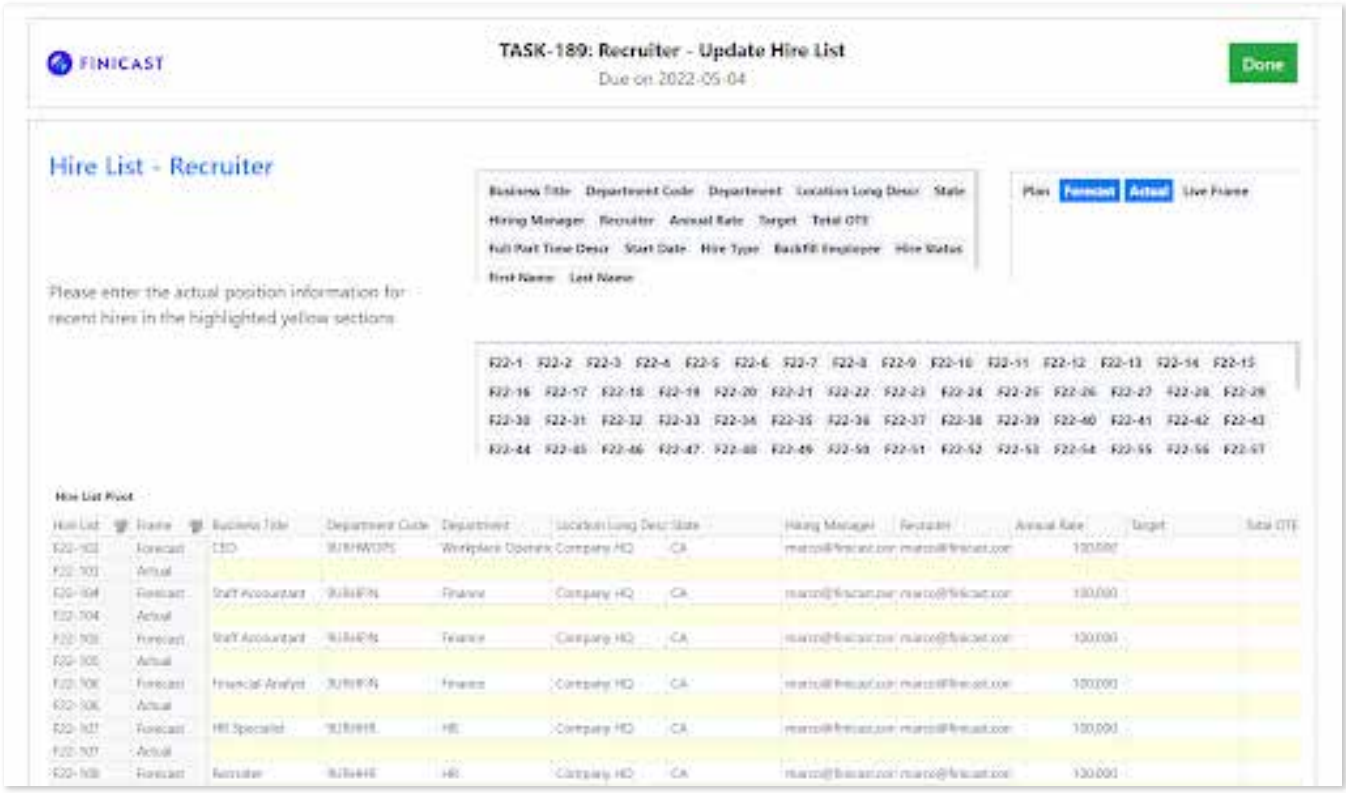


Finicast will prompt a user to log in for access to the task and the bidirectional dashboard.

The application requires the user's identity to access the dashboards and removes the risk exposure in sending out spreadsheets.

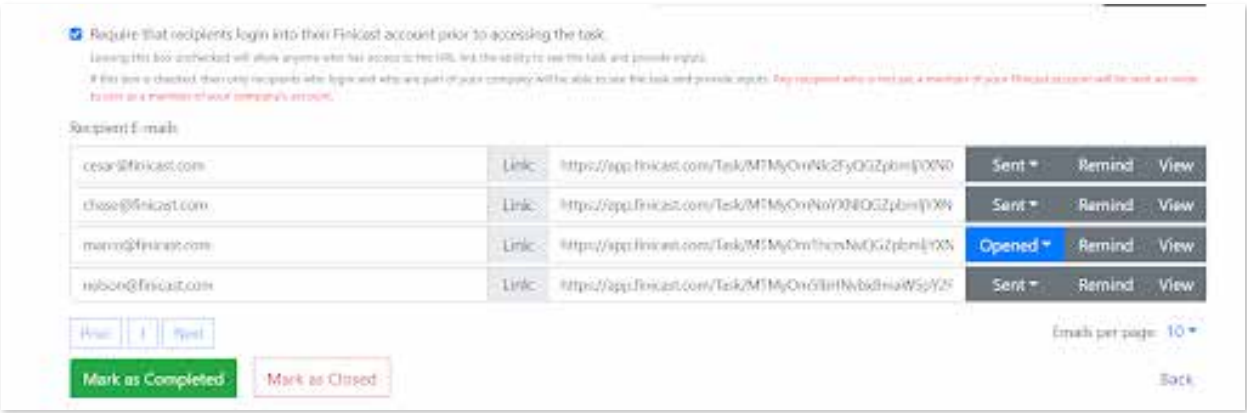


As defined by the task assignor, a logged-in user only sees what is relevant to them. Different users can access the same spreadsheet, all with customized views, eliminating the need for any additional spreadsheets to be created or sent out.



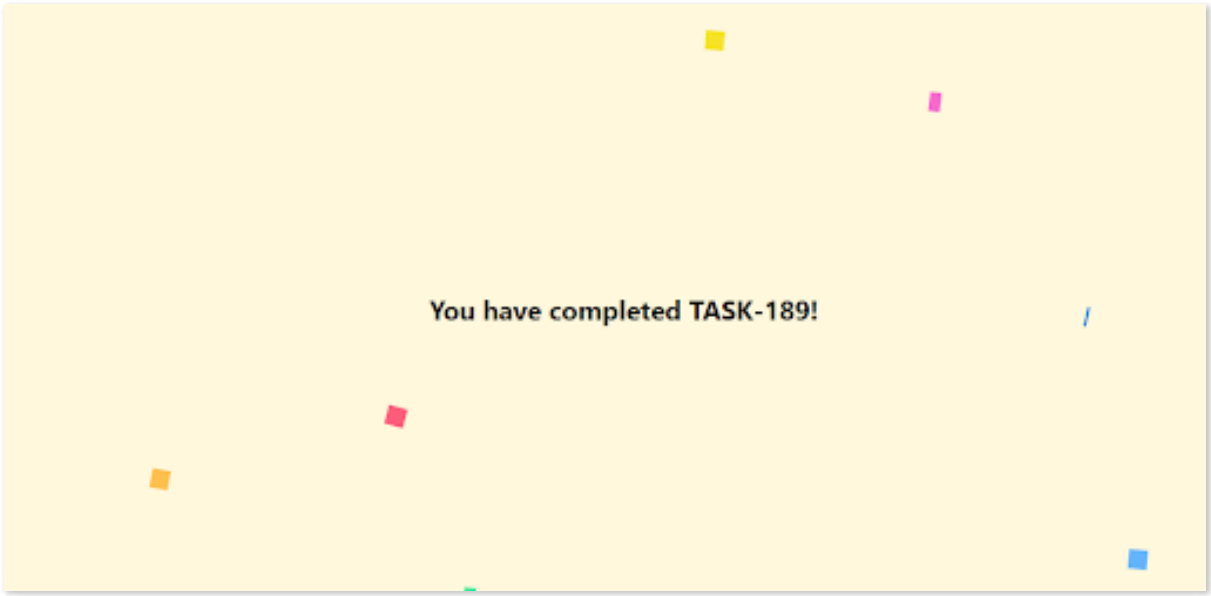
Monitor activity and revoke access as needed

Finicast offers the ability to “View As” the assigned user in a task. For example, the task assignor can view dashboards within a task by clicking “View" and validating that user's access.



Revoke Access Upon Task Completion

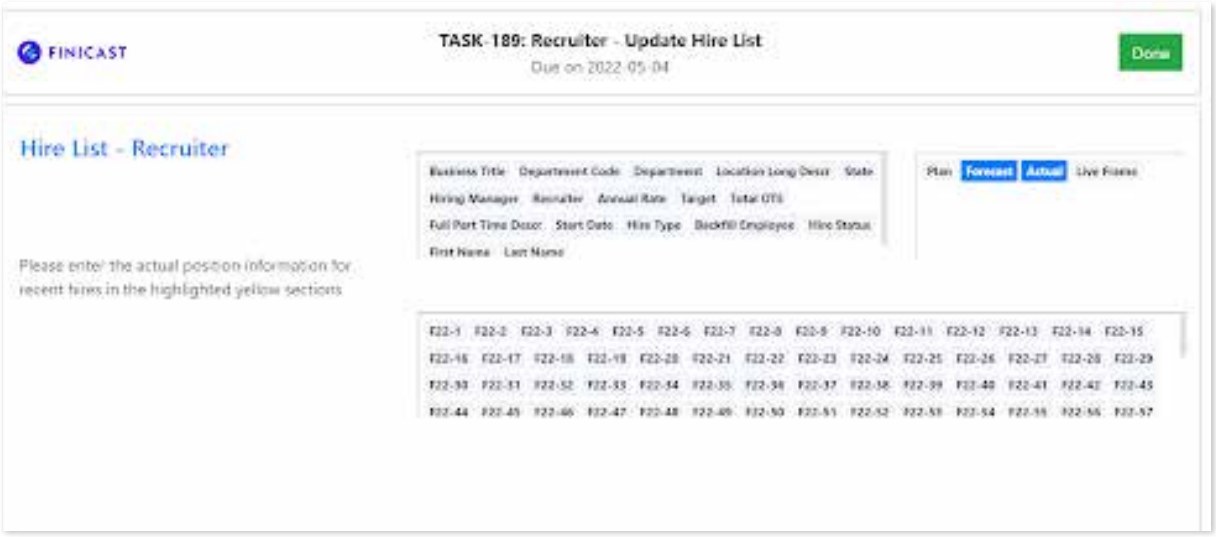
Once a user hits the “Done," the user will get the below notification on the web application. Trying to reopen the emailed link will result in the same completed task page.



Data is now reviewed by business users as needed per the task. Assuming a task is complete, access to business users can be revoked automatically.

Remove Improperly Secured Tables From Dashboards

If a dashboard does get sent out containing an improperly restricted table, simply remove the table from the dashboard, and all users with this task will no longer see that table.

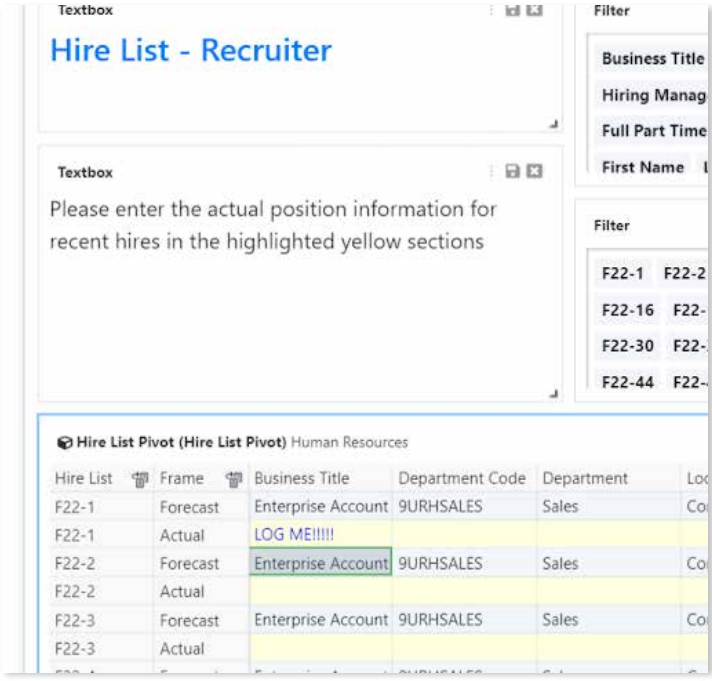


Log and Monitor Data Integrity

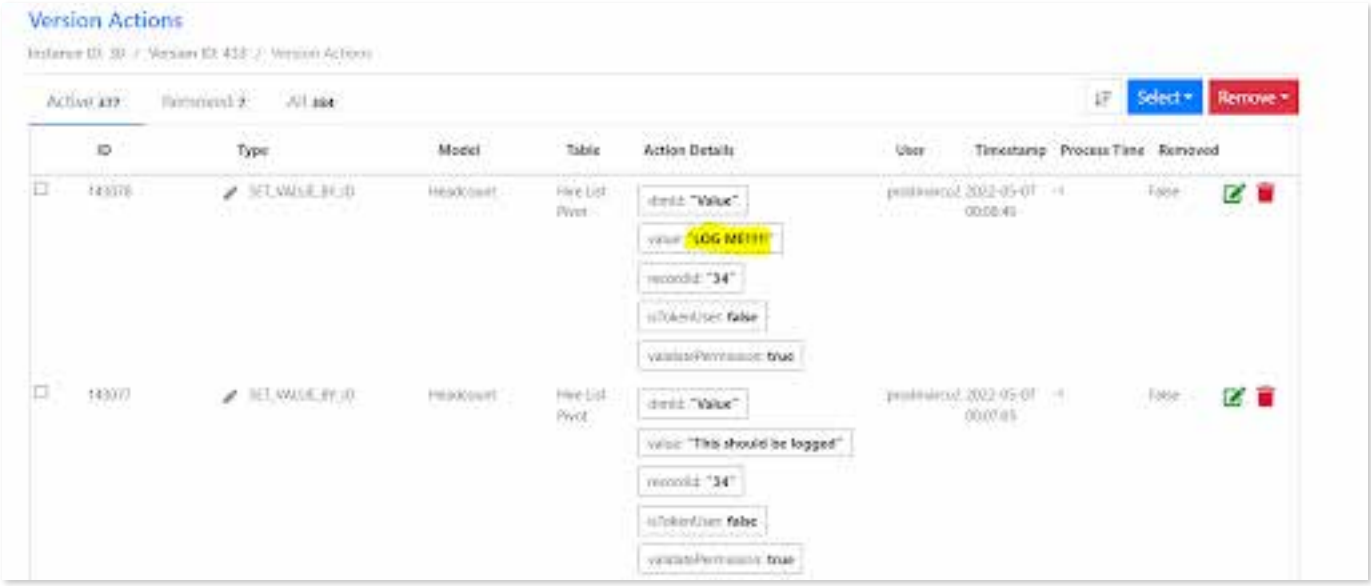
Finicast allows business users to set permissions for cells that can be edited, which are highlighted in yellow (input areas). This feature helps maintain the integrity of any data set and ensures that user mistakes do not compromise data or formulas.

As an additional security feature, a log of all actions completed on every table is kept within Finicast, allowing users to monitor and review data changes.

The below screenshots show a user commenting, "LOG ME!!!!!"



This action is logged in history, associated to the user, and timestamped. An audit trail begins the moment users start using Finicast.



Finicast as a Spreadsheet Solution

Finicast allows organizations to keep it simple and keep data secure.

This solution removes the need to manage multiple spreadsheets across the organization, limits the exposure of spreadsheets leaving the company, and safeguards against unauthorized access to data with a few clicks.

Finicast can enhance your company's security posture against the known risks of sharing traditional spreadsheets. Click here to subscribe to the Finicast newsletter and learn more about the tool.

Disclaimer
The information contained in this document is for educational and informational purposes only. This document is not intended to provide legal or regulatory advice and is provided "AS IS" without warranty of any kind. Organizations should engage appropriate legal, business, technical, and audit expertise for the review of regulatory compliance requirements.

Schellman
The statements and opinions stated in Schellman's section of the document are the opinions of Schellman Compliance, LLC ("Schellman"). Schellman does not opine on Finicast's capabilities and whether its features or controls meet any particular security requirements. Additionally, Schellman does not endorse or make recommendations regarding the use of any particular product or technology.

Finicast
This document is intended to provide general guidance for organizations that are considering Finicast solutions to help them address security requirements. The information contained in this document is for educational and informational purposes only. This document is not intended to provide regulatory advice and is provided "AS IS"