# Managing Security Access
# for
# SP Marketplace Products

## Copyrights and Trademarks



## Contact SP Marketplace

Email: info@spmarketplace.com

Postal Mail:

**SP Marketplace**
17319 Penn Valley Drive
Penn Valley, CA 95946

Website: www.SPMarketplace.com

Support: www.SPMarketplace.com/Support

Email: support@spmarketplace.com

# Table of Contents

## Overview

This document is a primer for administrators to understand security design of sites built with SP Marketplace products. The security is implementation must be fully understood before any customizations are done after the initial installation. The general security structure (access permissions in SharePoint terminology) for sites, lists and libraries will be discussed including the standard permissions setup configured during Installation of our OOTB products.

Guidance will be provided on the ramifications of making security changes to the default structure and considerations that must be made in administering permissions. This document applies to all SP Marketplace products except the HR Suite of products which is unique and covered in separate documents.

While customization may be applied to any of our products to implement Item Level Security for some lists or libraries, only the OOTB HR Suite of products have Item level security setup out-of-box. Item level security is more complex and difficult to manage but that level of security is required to secure confidential and private information that is normally the case with Human Resources products.

Overall management of security is a customer responsibility. SP Marketplace will not provide any security administration such as for maintaining SharePoint groups and their members, authentication and management of users and passwords, or managing external users. SP Marketplace will provide advice such as that contained in this document, the guidance during the customer QuickStart meetings, as well as the first-time setup instructions in the individual product Getting Started web pages.

## Assumptions

N/A

## Related Documents

Here is good detailed chapter from a book in the Microsoft Press library that has step by step details on permissions management from creating groups to breaking inheritance.

Security within SharePoint 2013

Microsoft Office/365 support contains this article on managing lists and library permissions:

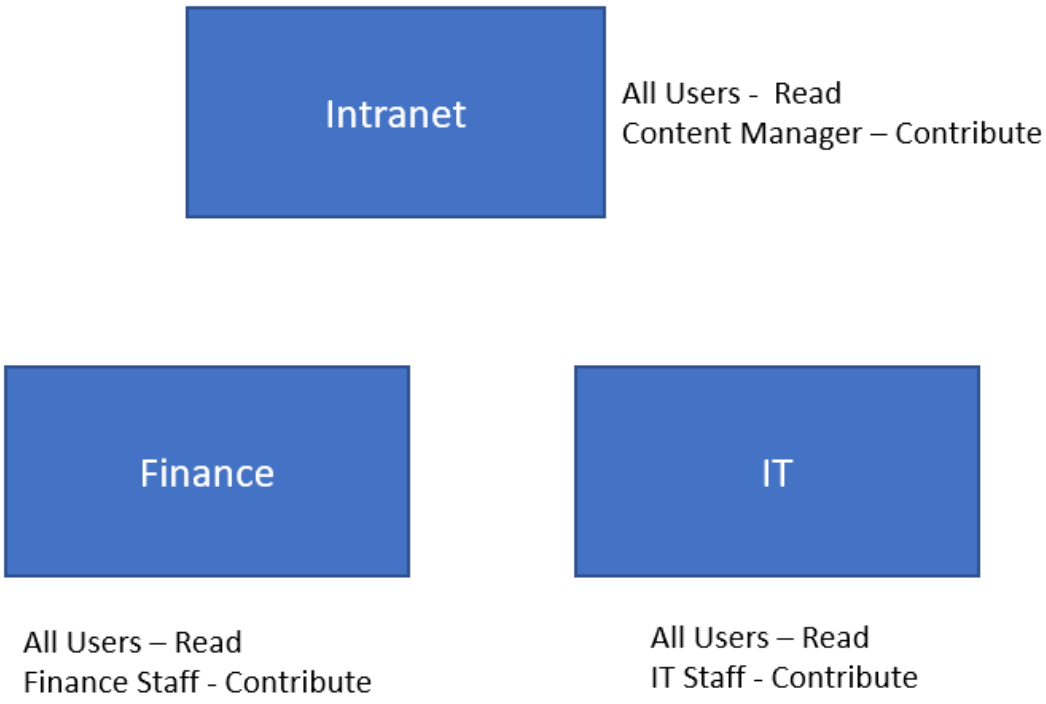
Edit and manage permissions for a SharePoint list or library

## Site Level Access/Permissions

When you create a new site in SharePoint, the default Site Permissions for the new site is to inherit the permissions from the parent site. When we create SP Marketplace sites during installation we do not use this default and instead designate that each site has unique permissions. Here is an example that illustrates why that approach is used.

In this example we have an Intranet product and 2 departments installed as subsites of the Intranet, a Finance department build using our generic Department Portal product and an IT department built using our IT Portal product. All SP Marketplace sites are installed with a SharePoint group called, SPMP Admin, which is given Full Control and should be populated with the SharePoint user ids of the customer administrators in addition to the SP Marketplace SharePoint user id provided on the customer tenant. To simplify the examples, the SPMP Admin group will not be included throughout the rest of this document and is NOT included in the below diagrams because it will always have full control.

When the products are installed, the All Users group is intended to include all SharePoint users except for external users so that SharePoint group will include the special SharePoint group, Everyone but External users as its contents. What that means is that there will be no need to add any specific users to that group. Note that normally SharePoint groups cannot include other SharePoint groups, the special SharePoint group Everyone but External users is one of the exceptions to this restriction. The diagram below is a simplified picture of these three sites where Finance and IT are subsites of the Intranet site and show the default out-of-box groups (except for SPMP Admin) specified in the Site Permissions.



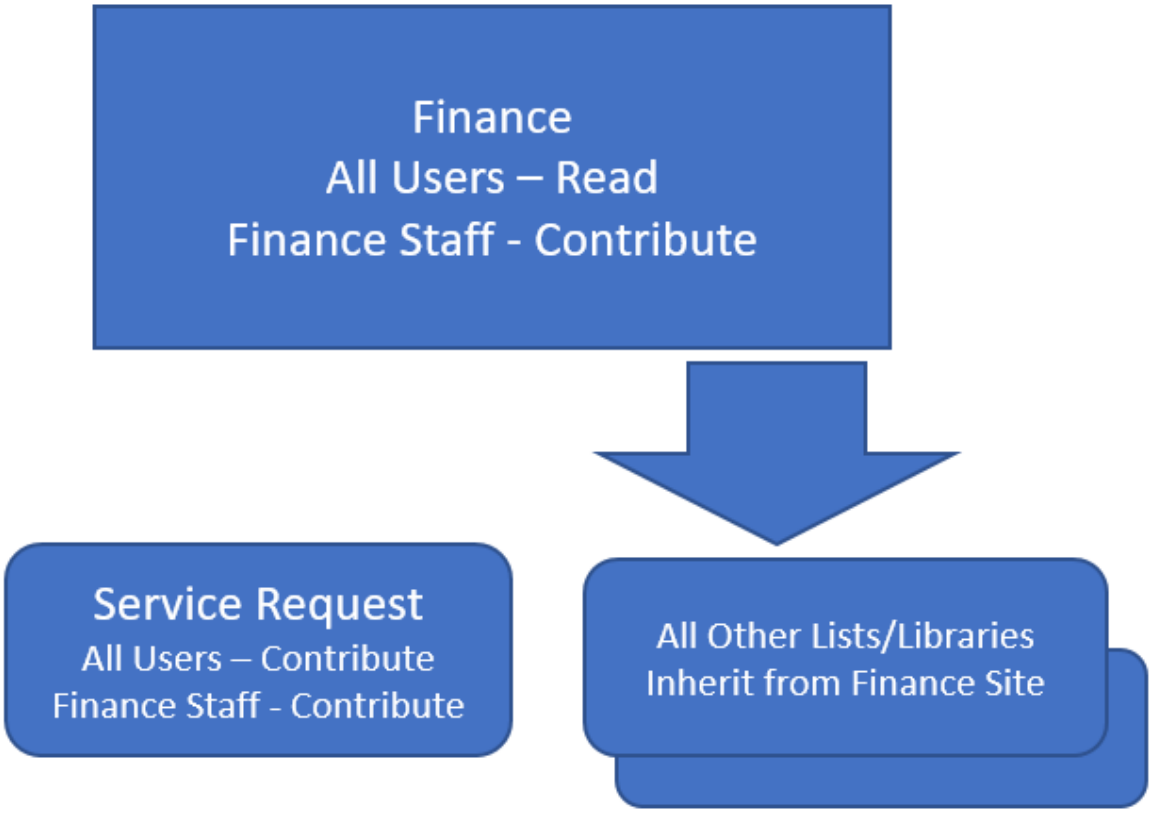

This illustrates why each site needs unique permissions and cannot inherit permissions from its parent site. The user group for managing the content of the Intranet is the Content Manager group which is unique set of users from the members of the Finance Staff group which are typically all the people in the Finance department. Further, the members of the IT Staff group are typically all the people in the IT department.

## List Level Permissions

Finance site permissions will be used to illustrate List Level Permissions, but the concepts presented apply to all other SP Marketplace products as well. At site creation time, the default site setup for all lists and libraries is to inherit the permissions that are set at the site level. However, there are some lists that need a different set of permissions than the site level permissions.

An example of that is the Service Request list in the Finance site. For all users to be able to create and modify their own service requests they need to have Contribute level access to this list. In SharePoint terms this means that the inheritance from the parent (site) must be broken and then the permission changed for the Service Request list. A detail step by step guide on how to do this is included in the appendix. This change is made during the installation of the SP Marketplace Department Portal site, Finance in this case.

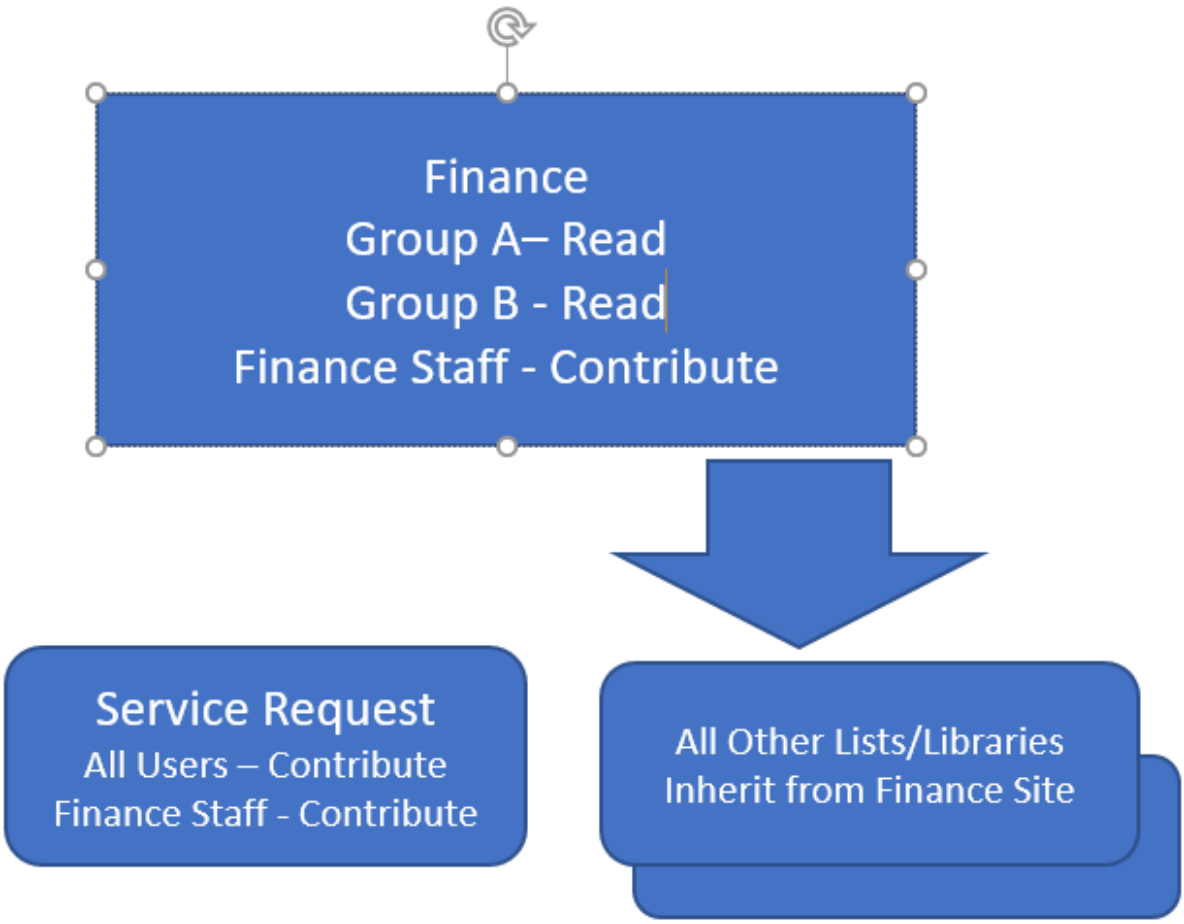
The below diagram shows this structure where the Service Request list no longer inherits permissions from the site and has unique permissions. There are two other lists and libraries in the Department Portal product (the Survey and Images library) that also have broken inheritance – they are not included in here to simplify this document. There is an appendix to describes the step by step details on how to determine which lists and libraries have unique permissions in a site.



## Change Management Considerations

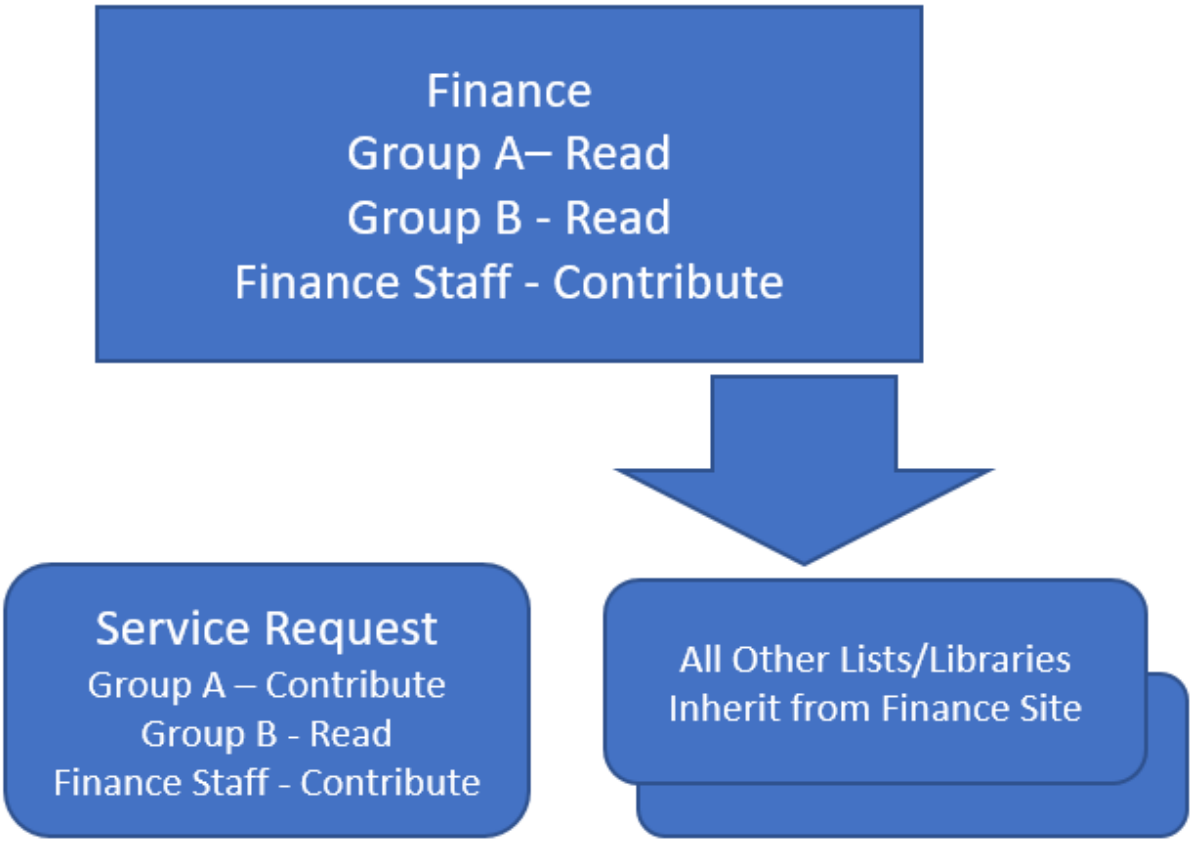
The are no security complications if all changes are made within the default groups above. Adding or removing users to these groups, All Users, Finance Staff, and SPMP Admin (not shown) is the normal way to manage permissions. Complications do arise when changes are made to the group structure. The following example illustrates the kind of problem that can occur when changing the group structure when there are lists that do NOT inherit from the site.

Instead of using one All Users group, you want to have 2 groups, Group A that will contain a list of users that can create Service Requests and Group B that can only read Service Requests. So, you create two new groups, Group A and Group B, in the Site Permissions and remove the All Users group from the site permissions. Here is what the permissions structure would look like:




Since the Service Request list no longer inherits from the Site Permissions this change does not work. Each list and library that no longer inherits from the Site permissions must be changed individually to receive the new Site Permissions.

Continuing with this example, the unique permissions in the Service Request list would need to be changed by removing All Users, and Adding Group A and Group B. Now that the permissions have been corrected the settings look like this:



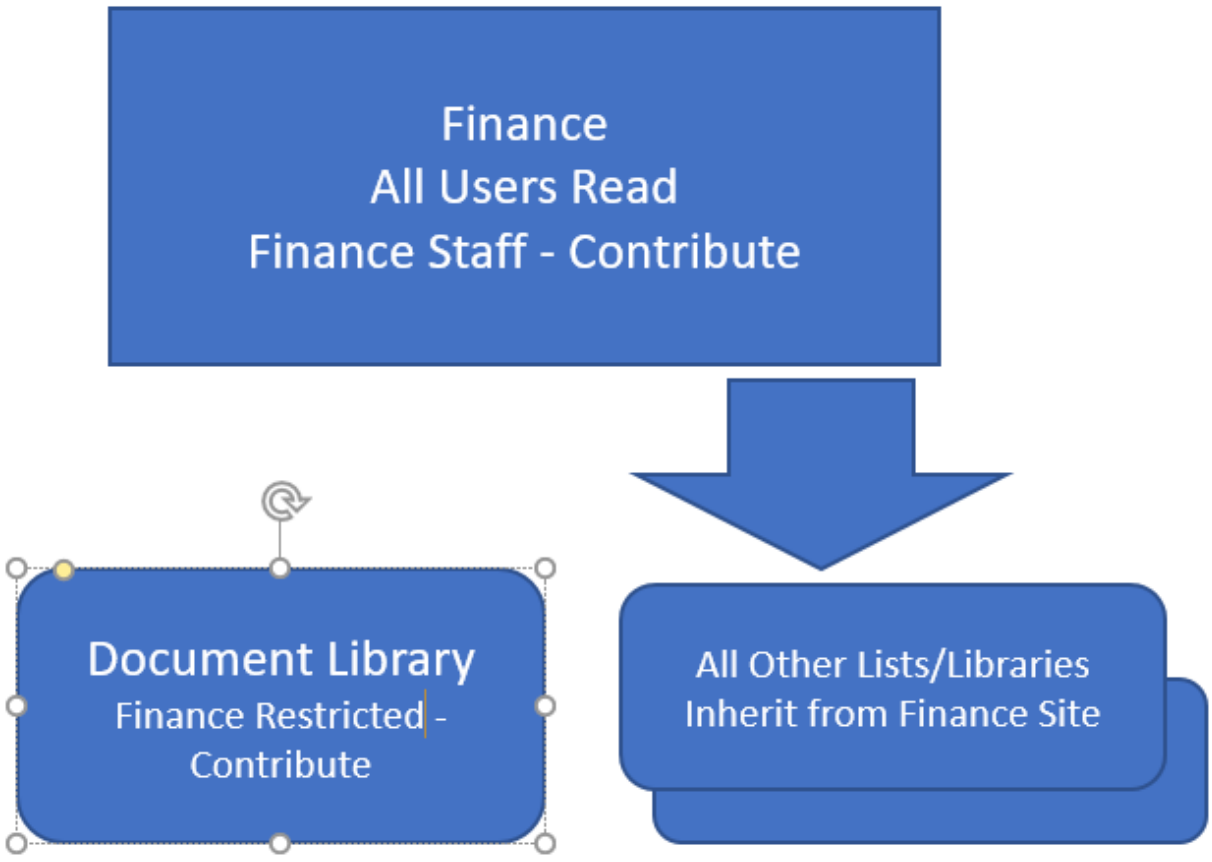

Conclusion: Whenever any changes are made to the site level permissions, such as adding new groups, and adding individual users, each list and library that no longer inherits permissions must be evaluated and probably its unique permissions changed.

## Tightening Security for individual lists and libraries

As part of the structure of all products (except the HR Suite which has enhanced security), there is an End User Portal page which the user is redirected to when accessing the site. This page limits visibility to the site, for example, the user sees only their own Service Requests. However, this is only a usability feature and does not prevent these end users from accessing (limited to read) all lists and libraries in the site by using Site Contents or direct URLs. In some cases, you will need to provide tighter security for some lists and libraries in the site.

Here is an example using our Finance Site. Assume that the document library which is NOT visible thru the End User Portal page (but again can be accessed thru Site Contents) contains sensitive information such as P&L statements and you need to restrict it to even a smaller group of people than the Finance Staff. To solve this, create a new group, Finance Restricted which contains a subset of the Finance Staff group.

Since that group is a subset of the Finance Staff group, there is no need to make changes to the Site level permissions. What you will need to do is break the permissions for the target (P&L) document library, remove the All Users and Finance Staff Group and add the Finance Restricted group. The diagram below shows how this looks, with the Service Request list removed which remains unchanged in this example.

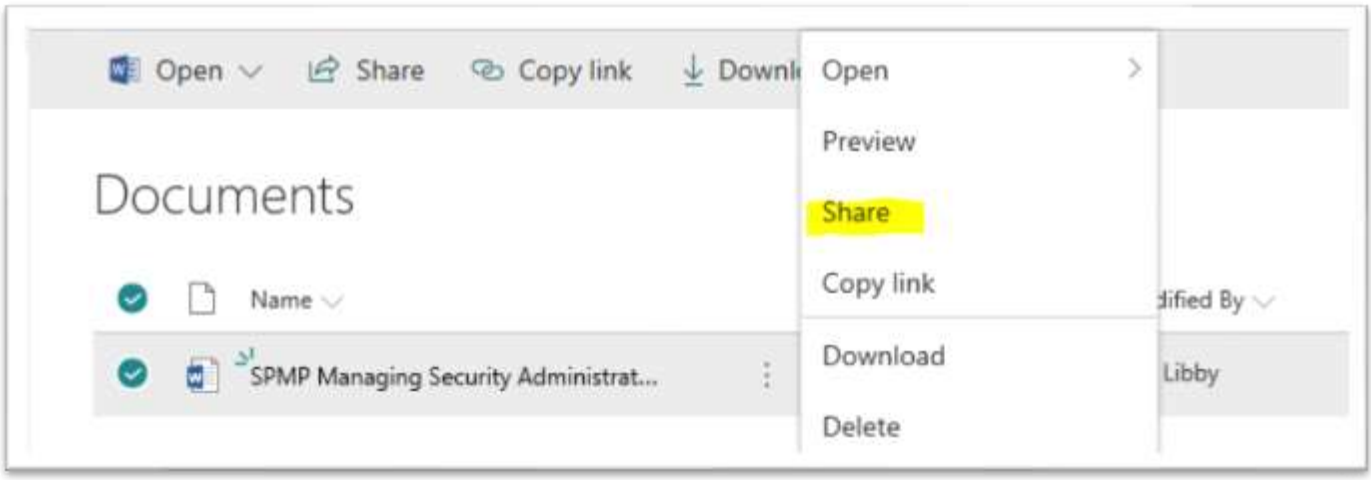



Now the only people who can read or contribute to the Document library in the Finance site are members of the SPMP Admin and Finance Restricted group. Again, SPMP Admin group is not shown in any of the diagrams for simplification purposes.

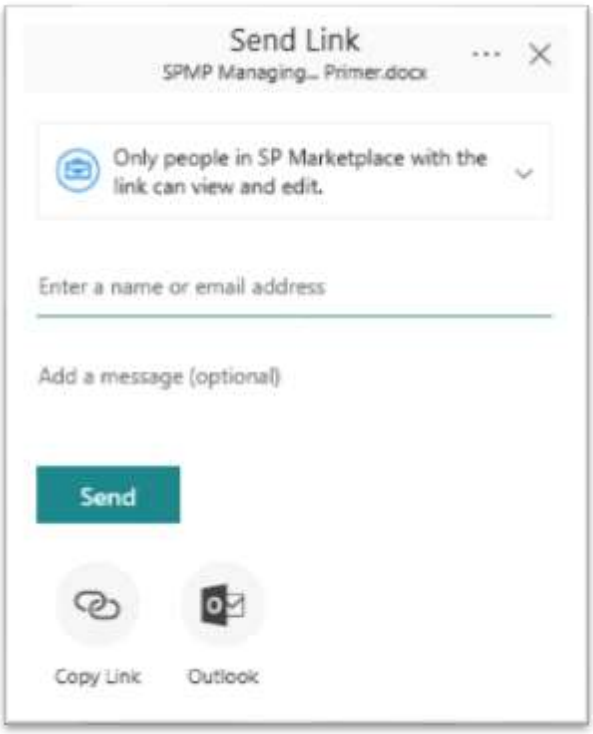
If you decide to maintain two separate groups (Finance Staff and Finance Restricted) where the Finance Staff does not include all the people in the Finance Restricted group, and visa versa, then change the Site Permissions to include Finance Restricted and more importantly add the Finance Restricted group to all the lists and libraries (like the Service Request) that no longer inherit permissions from the site.

## Item Level Security

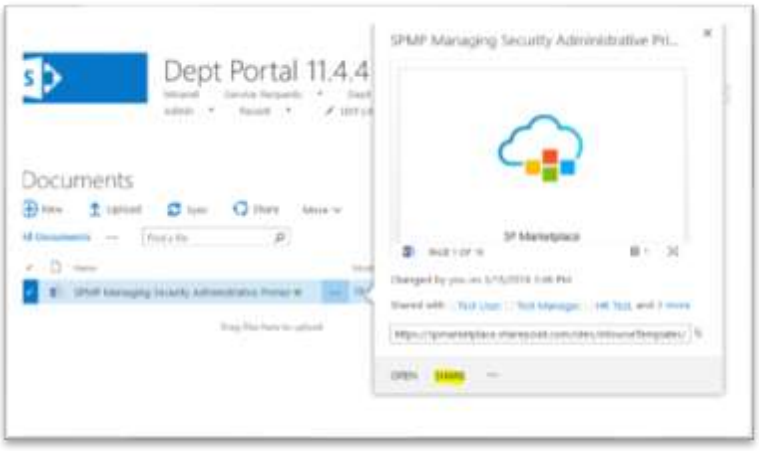
Because only the HR Suite of products implements Item level security, details of managing security across the HR Suite of products will be covered in a separate document. However, there is a case where item level security is created in a non-HR site, and it may not be obvious this is happening. This is most likely to occur in document library when Share from is selected from the ellipses menu as seen from the Modern UI.



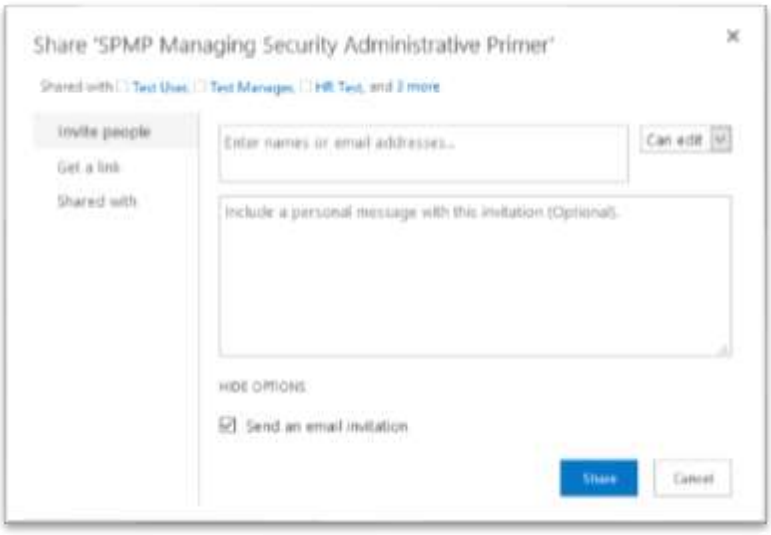

Clicking on Share allows you to Share this document with a user or group and send them a direct link to the document.



In the classic experience you can accomplish the same by first using the ellipse menu (…) for a selected document you click on Share in the popup box as shown below:




Then you will get the dialog box below which allows you to Share this specific document with a Sharepont Group or User and optionally send them an Email.




So where do the problems occur here – well since you can share this document with SharePoint users who are NOT in the permissions list for the library this action results in breaking the inheritance of permissions from the document library and this document then has a unique set of permissions. It will have the current permissions from the Document library and the new permission added by the Share action – that document will then have item level permissions that are different than the Document library level permissions and it will no longer inherit its permissions from the Document library.

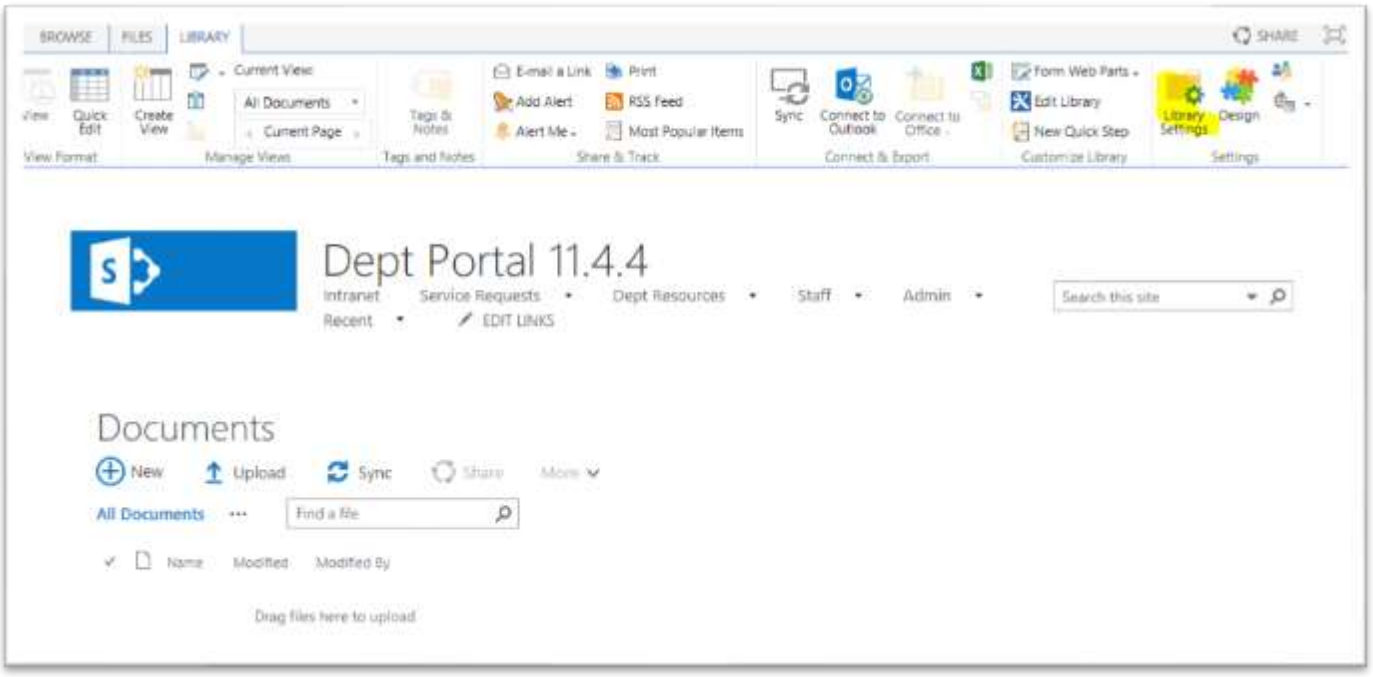
If the Permissions for the Document Library are not changed this process likely will not cause any issues. However just like Lists and Libraries unique permissions discussed above the same issues exist for unique item/document level permissions. For example, if a new group is added to the permissions list for the document library the users of that group will NOT have the same permissions in all documents in that library that have previously been changed to not inherit from the library permissions.

# Appendix

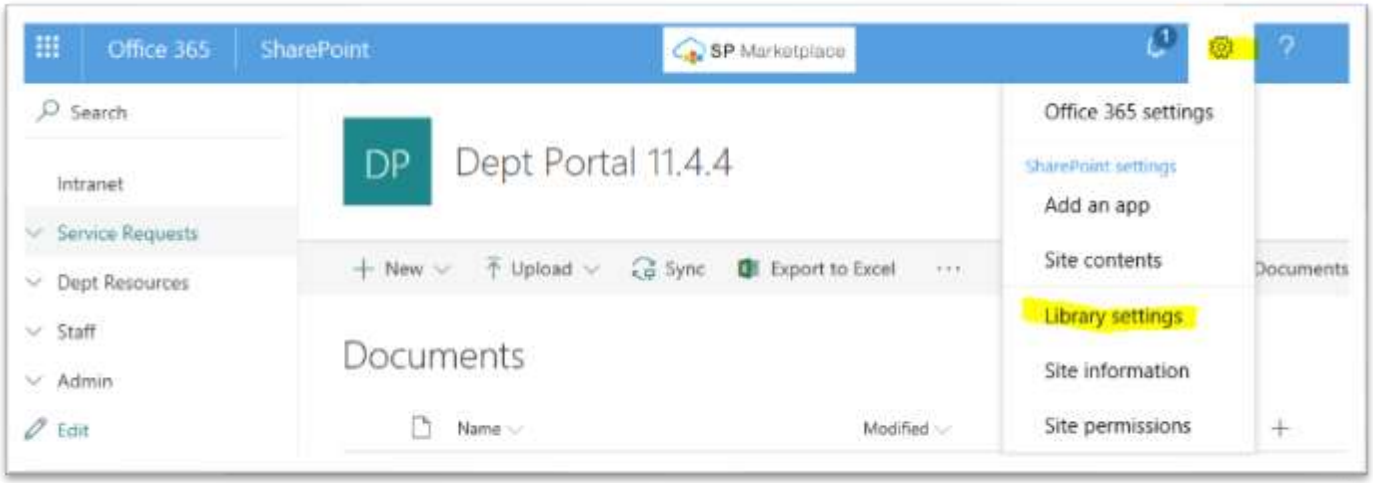
## Changing List level permissions

In order to change the list level permissions so they are different than the site level permission, the first step is to Break the Inheritance Structure. First go to the settings for the list or library. You do this by clicking on List Setting or Library Setting in the SharePoint ribbon while using any view in that list and Library.

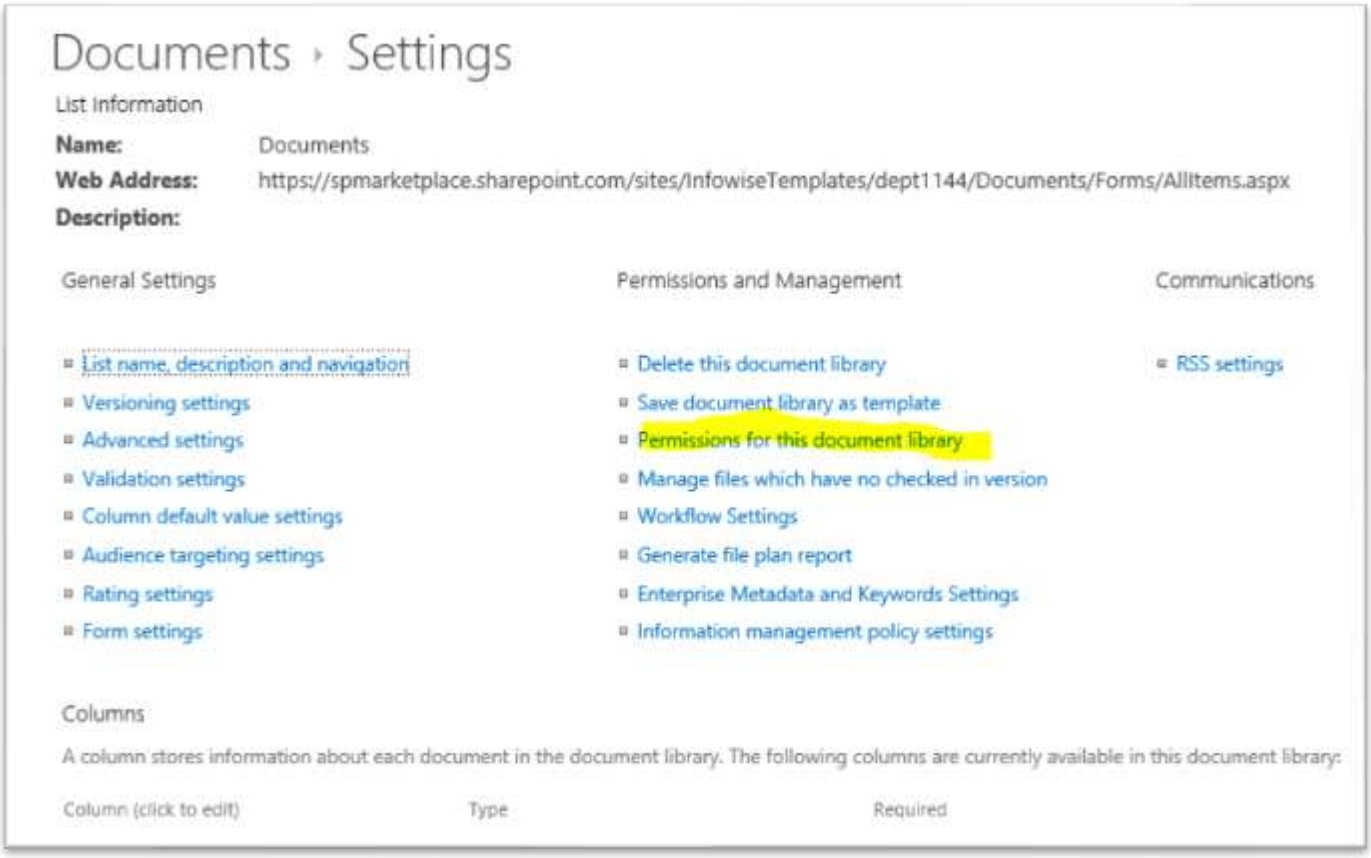
Example for Document library below using the classic UI.



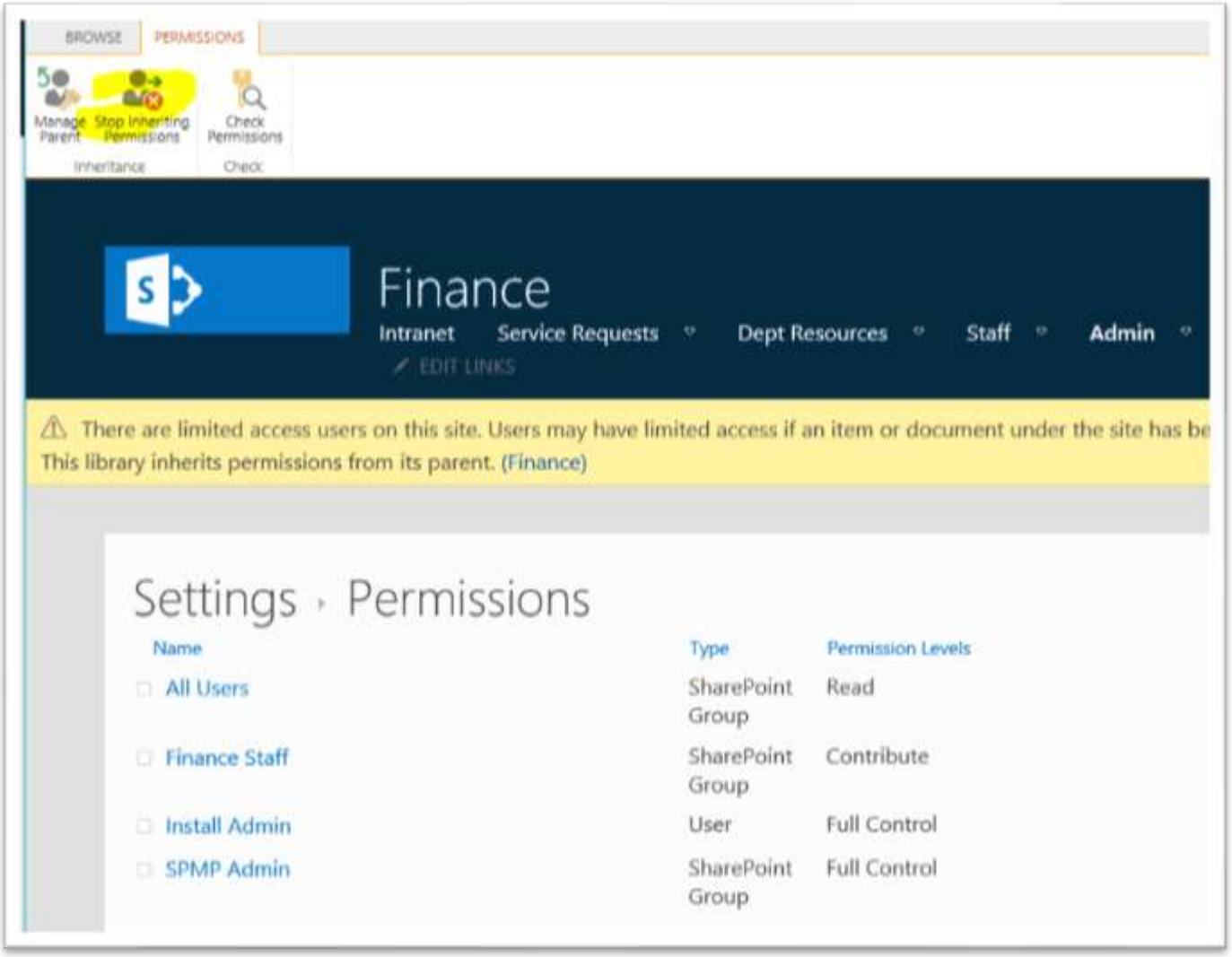

Using the Modern UI for the same document library use the wheel as shown below:



Once in the Library or List Settings click on Permissions for this document library (or List) as shown below:

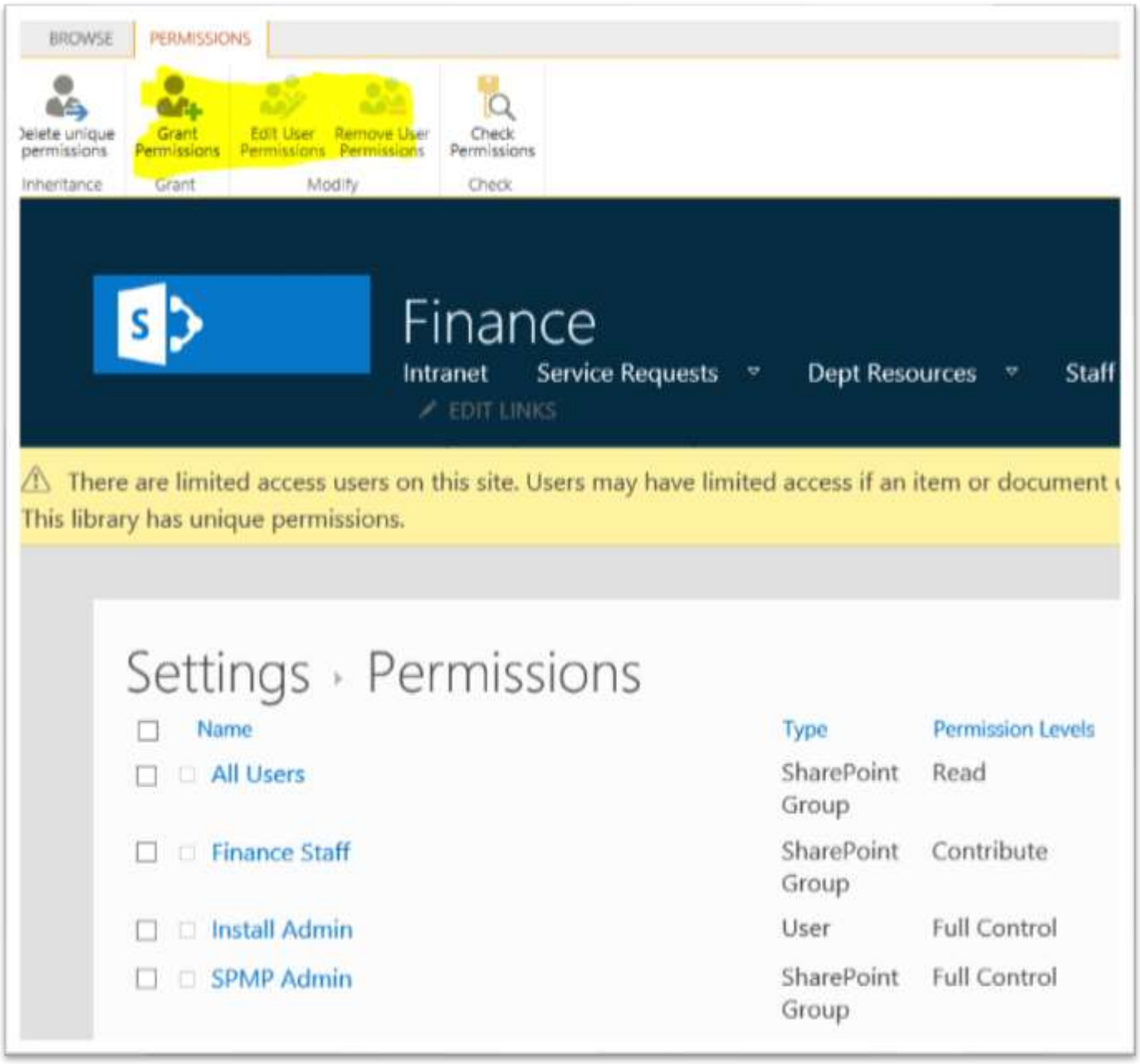



Now before you can change the permissions on the list and library (remove a group or add a new group or change the permission level of a group) you must first Stop Inheriting Permissions as highlighted below.




Click OK to the warning popup message below:

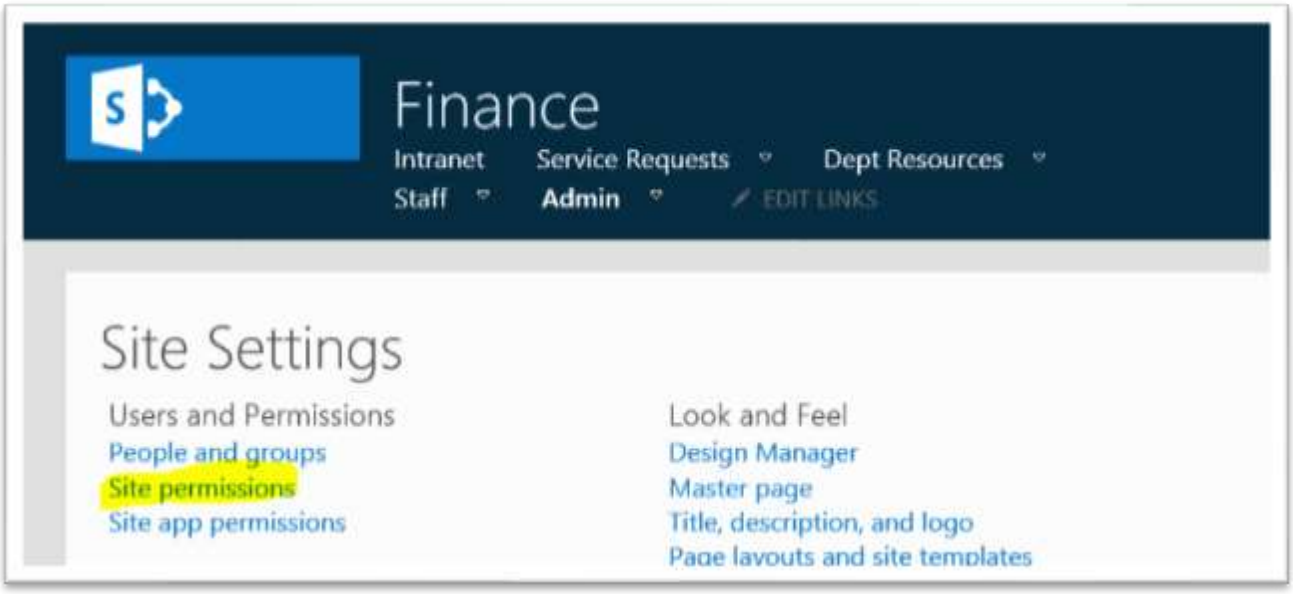
Then you will see the following new actions highlighted below which will allow you to add new groups or individuals (we recommend ONLY using groups), change the Permissions of existing groups or remove existing groups completely.



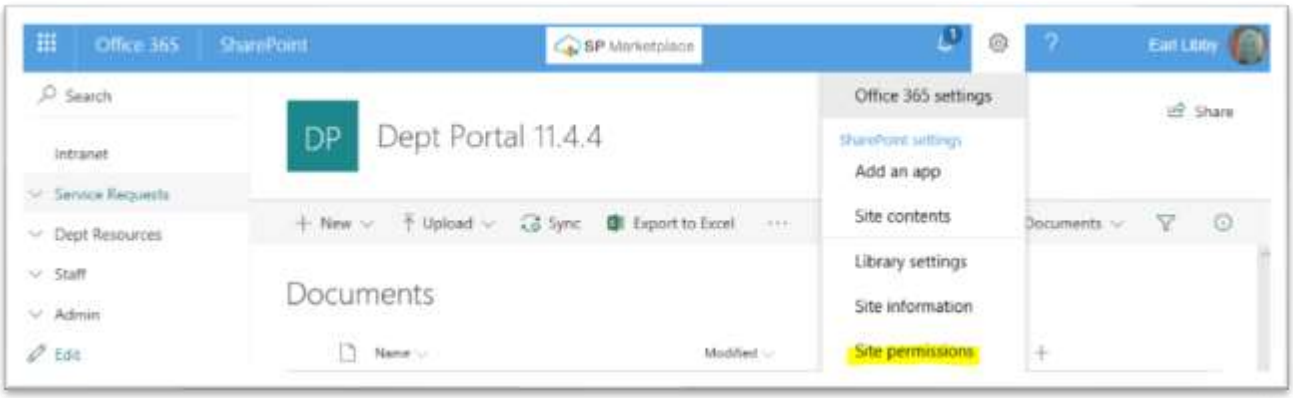
## Finding and managing Lists and Libraries that do NOT inherit site permissions

When managing any changes to Site level permissions it is critical to understand what lists and libraries do not inherit from the Site Level Permissions so that you can if needed change the unique permissions on each list not inheriting.

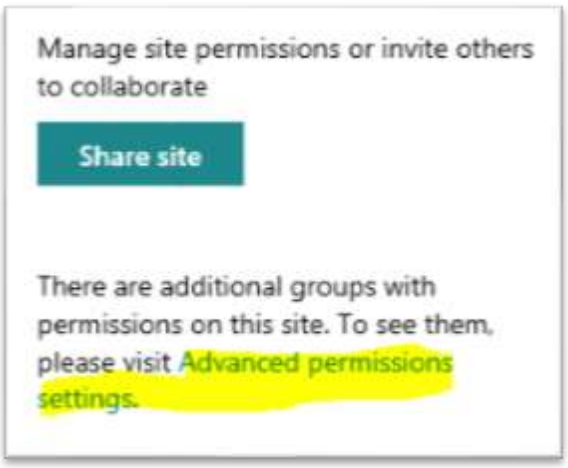
First go to the Site Permissions for the site to do that select Site Setting from the wheel in the upper left corner and click on Site Settings, then click on Site Permissions as shown below:



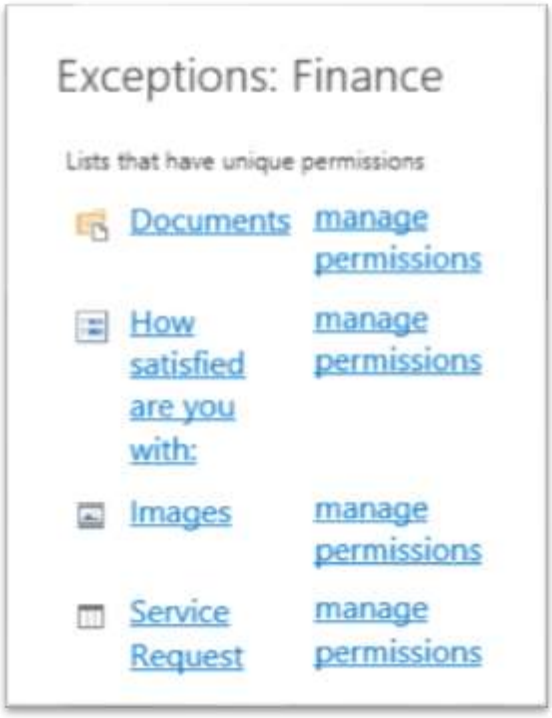

Or when using the Modern UI you click on the Site Permissions from the wheel as shown below:



Then select advanced Setting in the popup box:




Using either approach now you can see all the permissions for the site and as highlighted below that will indicate if there are lists or libraries that have unique permissions. Click on Show These Items and you will get the following:




And the Manage Permissions takes you directly to the Unique Permissions dialog box for that list or library.

Note: in the above List/Libraries that have unique permissions, the Survey, How satisfied are you with, Images and Service Request are configured with Unique Permissions as part of the installation. The Documents library is unique because permissions inheritance was stopped after install which happened as part of the previous appendix example.