Performing an IT Separation of Duties Analysis

Desk Procedure

Version 1.0

July, 2021

Contents

1 Overview

In principle, Separation of Duties (SOD) is a methodology used to identify and prevent conflicts of interest wherever defined user roles exist throughout a business enterprise. For example, work performed by one person should be approved by another person. Implementation and use of a SOD ensures the integrity of the work performed by a business unit, thus preserving reputational standing and reducing the possibility of legal action brought against the business. SOD applies to many areas of business activity, such as sales, human resources, IT, accounting, etc. Red Hat requires implementation of a SOD across and within all business units.

This manual details how a business manager or other authorized Red Hat associate can apply a SOD Matrix to facilitate identification of potential conflicts and expedite compliance with Red Hat SOD requirements.

2 Getting Started

The Red Hat SOD Matrix is a generic template that can be customized to the needs of the business unit. The matrix contains multiple tabs and corresponding spreadsheets that facilitate the creation of a business-specific matrix. In Google Docs, the matrix can be renamed according to the operational name of the business or any other preferred naming convention. A copy of the template can be downloaded here.

2.1 Universal IT SOD Matrix

For IT operations, the SOD Matrix template features a **Universal IT SOD Matrix** tab and corresponding spreadsheet that allow an IT professional to identify at a glance the user roles that apply within the business unit. Fifteen defined roles appear from left to right across the top of the matrix along the x axis. These roles are repeated from top to bottom on the left along the y axis. Wherever a named user role intersects with a conflicting function along the axes, an **X** appears to signal the conflict.

Note: Where a user role intersects with itself on these axes, a grey field appears to signal role redundancy.

Red Hat

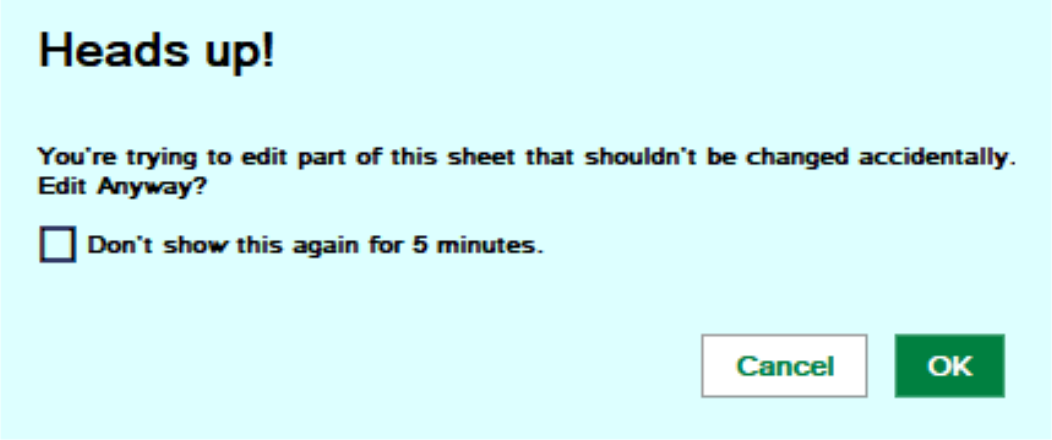
Separation of Duties [ANY-APPLICATION]

Note: below are the universal IT tasks. You should keep the IT tasks that are applicable to the application and delete those not applicable.

Based on the job responsibilities and the application role/ responsibility setting, RH identifies the following SOD conflicted tasks:

IT Task Description		1 Develop code	2 Configure application	3 Perform unit test	4 Perform UAT	5 Code review	6 Approve change (code, configuration or patch)	7 Promote change to the production environment	8 Approve User Access	9 Application User Admin - access management (add/delete user)	10 Application Role Admin - role access management (add/delete entitlements within the role)	11 Configure batch job	12 DBA - Perform Database Management Activities	13 Database - direct data change at the back-end	14 O/S root access	BU Perform Business User (BU) tasks (not read access) in the production application.	Application Roles	Example: Oracle Application Roles
Develop code	1			X	X	X	X	X		X	X	X	X	X	X	X		N/A, Oracle developer team
Configure application	2			X	X		X	X		X	X	X	X	X	X	X		None
Perform unit test	3	X	X				X	X										N/A, Oracle developer team
Perform UAT	4	X	X				X	X										N/A, business user, normally the change
Code review	5	X																N/A, Oracle developer team peer review

Note: The Universal IT SOD Matrix is write-protected to generate an alert if a user attempts to edit matrix field contents.



2.2 Applied IT SOD Matrix

The SOD Matrix template also features an **Applied IT SOD Matrix** tab that allows an analyst to create a SOD spreadsheet according to defined roles or by assets.

Red Hat

Separation of Duties [ANY-APPLICATION]

Security Warning Data connections have been disabled Options...

E6

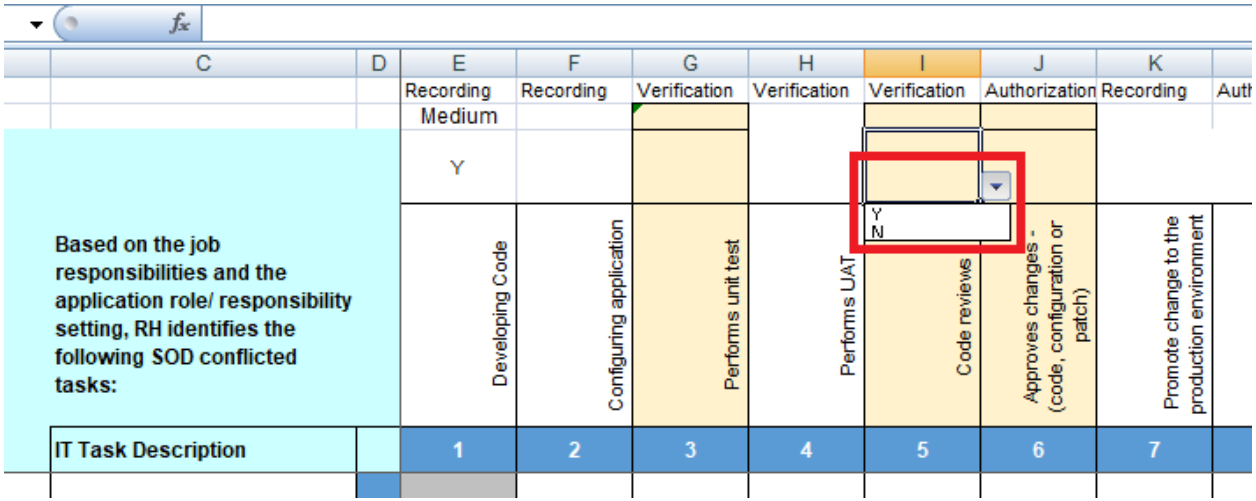
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1					Recording	Recording	Verification	Verification	Verification	Authorization	Recording	Authorization	Recording	Recording	Recording	Recording	Recording	Recording	Recording
2					Medium													Critical	
3					Y													Y	
4			Based on the job responsibilities and the application role/ responsibility setting, RH identifies the following SOD conflicted tasks:		Developing Code	Configuring application	Performs unit test	Performs UAT	Code reviews	Approves changes - (code, configuration or patch)	Promote change to the production environment	Approve User Access	Application User Admin - access management (add/delete user)	Application Role Admin - role access management (add/delete entitlements within the role)	Configure batch job	Perform Database Management Activities - DBA	Database - direct data change at the back-end	O/S root access	Perform Business User (BU) tasks (not read access) in the production application.
5			IT Task Description		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
6	Medium	Y	Develop Code	1														M/C	
7			Configure application	2															
8		0	Perform unit test	3															

Generic SOD | Universal IT SOD Matrix | Assets | Checklist | Applied IT SOD Matrix | RoleUser | Analysis by User | Ass

Ready 80%

Row 3 of the matrix features a drop-down series of yes/no responses to questions that appear in row 4. The answer selections made to each question determine the **Criticality Index**, if any, associated with each role. For a discussion on how the Criticality Index works, see §2.5.

Note: Yes/No drop-downs are expressly for use when the questionnaire cannot identify the value. When a selection can be made, the headers are almond in color. When a selection cannot be made, the headers are white.



To prepare a SOD according to assets, the template includes an **Assets** spreadsheet that lists suggested assets, detailed in §2.3.

2.3 Assets

The **Assets** tab of the SOD Matrix template contains an interview style spreadsheet designed to facilitate identification of business assets and who is responsible for producing them.

Note: For the purposes of SOD, an asset is any product or service produced by the business unit.

Red Hat

Separation of Duties [ANY-APPLICATION]

A1 | Suggestions of Assets You Might Produce

	A	B	C
1	**Suggestions of Assets You Might Produce**	**Assets - What does your team produce**	**Who does the work (Idea Session)**
2	Code	Automation Script	Developer, QA, UAT, Release
3	Infrastructure (Connections)	Automation Infrastructure (Connections)	Architect, Support
4	Reports	Automation Results	User
5	Release Management	Automation Release Management	Developer, QA, UAT, Manager
6	Security	Automation Security	Developer, QA, Security
7	Education	Automation Education	Developer, Support
8	Desk Procedures	Automation Desk Procedures	Support
9	Novel Idea	Automation Novel Idea	Developer, Architect
10	Roles (Userids)	Automation Roles (Userids)	Business Owner, Manager, Access Manager
11	Infrastructure (Servers)	Automation Infrastructure (Servers)	Architect, Support
12	Disaster Recovery	Automation Disaster Recovery	Architect, Support, Developer, QA
13	Support (Userids)	Automation Support (Userids)	Business Owner, Manager, Access Manager
14	Problem Resolution Documents	Automation Support Activity	Support
15	Passwords repository	Automation Passwords in Hashicorp	Users
16	Architecture	Automation Architecture	Business Owner, Developer, Architect
17	Solution Platform	Automation Solution Platform	Business Owner, Developer, Architect
18	Service Now Tickets	Automation Service Now Tickets	Developers, Users
19	Key Reports	Automation Key Reports	N/A
20	Windows Environment	Automation Windows Environment	
21	Linux Environment	Automation Linux Environment	
22			
23			

Assets as Scoping Boundaries

The first scoping considerations involve assets. Duties that are related to a
long as they do not involve the same asset. This kind of SoD is allowed in s

Again, SoD may be accomplished on different levels. In some cases, segre
employees may be in charge of recording and authorizing transactions on
transaction's data and the other employee authorizes the operation.

In this case, if assets are, for instance, accounts receivable, two employees
single account receivable, one employee records the data and the other en
employees when a second account receivable is processed. The traditiona
manager) and custody or recording operations to a second individual.[16]

Therefore, the first scoping rule is that duties must be segregated for every
exchange their duties). More commonly, particularly in medium or large en
example, in which authorization for paying accounts receivable is perform

https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/imple

Next move onto Transformation

Processes as Scoping Boundaries

A second boundary may be created by the processes that transform the as

Generic SOD | Universal IT SOD Matrix | Assets | Checklist | Applied IT SOD Matrix | RoleUser | Analysis by User | Ass

Ready | 100%

Included in this spreadsheet (in column A) is a list of **Suggestions of Assets You Might Produce**. This list may include code, tutorials, release management guidance, etc. The list is an abstract of assets the business could, in theory, be responsible for. The list is not definitive, as each business will ultimately produce in practice a discrete mix of assets unique to the business.

Column B lists **Assets Your Team Produces**. This list includes the assets the business *actually* produces. The list reflects the scope of the business and can be modified as the mission of the business evolves. Items in this list should loosely align with the items in column A.

Column C lists the party or parties (defined by role) responsible for producing the asset listed in column B. Note that the roles and titles listed in column C can be used to populate the list of application users under the **Role/User** tab (see §2.6).

Note: Listed template content that is not relevant to the business can be deleted.

2.4 Checklist

The SOD **Checklist** spreadsheet poses precise SOD questions and corresponding answers delivered in a drop-down list format.

Column E of the checklist presents a list of 30 relevant questions.; **yes** or **no** answers can be selected from the drop-down list in column F. Column H features an extended discussion of these answers.

E	F	G	H
The purpose of the tab is to identify **all privileged access at different domains** across application and infrastructure layers for further SOD analysis			
	Initial Information Collection		
Checklist	Answer (all	Specify the info if column marked in Yellow	Explanation
Can RH manage the O/S directly?	Yes		Select answer from drop-down list at Column F. If Column F answer is Yes, **please specify the O/S name** Linux, OpenShift, Mainframe, Microsoft, etc.
Can RH configure the batch job?	Yes No		Select answer from drop-down list at Column F. If Column F answer is Yes, **please specify the type of th** column G.
Is a third party job scheduler tool used?	No		Select answer from drop-down list at Column F. If Column F answer is Yes, please **specify the tool nam** Cron, autosys, etc.
If item #5 answer is Yes, list all the individuals in column G or tab "Job Schedule Configurator" that can configure the batch job.			**List the individual names** in tab "Job Schedule Configur the procedures listed in the tab.

Red Hat

Separation of Duties [ANY-APPLICATION]

Security Warning Data connections have been disabled Options...

F4 | Type 1a

The purpose of the tab is to identify all privileged access at different domains across application and infrastructure layers for further SOD analysis

					Initial Information Collection		
Layer	ITGC Domains	Sub-domain	#	Checklist	Answer (all	Specify the info if column marked in Yellow	Explanation
General	General	General	1	Application type	Type 1a	[redacted]	**Select from one of the following in column G:** - **Type 1:** RH **can** make direct change to the **source code.** Custom software includes "home grown" systems as well as vendor provided systems for which the company has the source code (all or part). - **Type 1a:** RH cannot make direct change to the kernal source code (baseline). But can make customized changed to the **functions** of the applicaiton. - **Type 2:** RH **cannot** make direct change to the **source code**. RH **can** make changes to the **configurations, direct data update or programs (Python, etc) for data processing.** - **Type 3:** RH **cannot** make direct change to the source code and configurations.
Database	DB	DB	2	Can RH manage the database directly (change data structure, table, relation of the tables, etc.)?			Select answer from drop-down list at Column F. If Column F answer is Yes, **please specify the DB name** in column G. E.g. MariaDB, Mango, Oracle, etc.
		Direct data update	3	Besides DBA, are there users who can update data directly at back-end (e.g the database)?			Select answer from drop-down list at Column F. If Column F answer is Yes, please **specify the user names**.
O/S	OS	OS	4	Can RH manage the O/S directly?	Yes		Select answer from drop-down list at Column F. If Column F answer is Yes, **please specify the O/S name** in column G. E.g. Linux, OpenShift, Mainframe, Microsoft, etc.
	IT Operations	Batch job	5	**Can RH configure the batch job?**			Select answer from drop-down list at Column F. If Column F answer is Yes, **please specify the type of the batch jobs** in column G.
				Is a third party job scheduler tool			Select answer from drop-down list at Column F.

Generic SOD | Universal IT SOD Matrix | Assets | Checklist | Applied IT SOD Matrix | RoleUser | Analysis by User | Ass

Ready 80%

Note that answers in column F are correlated with a conflict criticality color, as follows:

- Green: no conflict (or, no criticality)
- Orange: moderate conflict (or, moderate criticality)
- Red: serious conflict (or, serious criticality)

2.5 Criticality Index

The Checklist is designed to automatically populate corresponding fields in the Applied IT SOD Matrix with a criticality value based on the answers selected. This allows the user to detect potential conflicts and take corrective action.

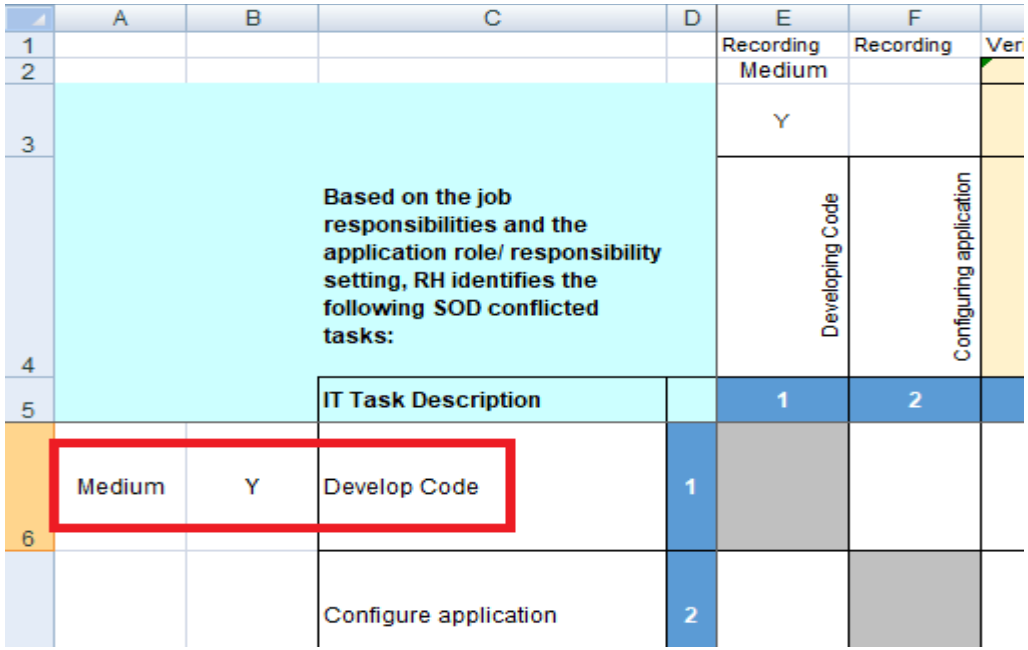
The Criticality Index assigns the following criticality values to potential conflicts within the Checklist:

- **L/L** = (**Low**) **Low** criticality: conflict poses a trivial risk that likely requires no remediation
- **L/M** = (**Low**) **Medium** criticality: conflict poses a minor risk that may require no remediation or only small adjustment
- **L/C** = (**Low**) **Critical** criticality: conflict poses a minor but substantial operational risk and should be evaluated for possible remediation
- **M/L** = (**Medium**) **Low** criticality: conflict points to a measurable operational risk that should be addressed as soon as practicable
- **M/M** = (**Medium**) **Medium** criticality: conflict poses a moderate operational risk that should be remediated without delay
- **M/C** = (**Medium**) **Critical** criticality: conflict poses an elevated operational risk that should be remediated at the first opportunity
- **C/L** = (**Critical**) **Low** criticality: conflict poses an operational risk that appears regularly and should be addressed promptly
- **C/M** = (**Critical**) **Medium** criticality: conflict poses substantial operational risk that should be remediated at the first opportunity
- **C/C** = (**Critical**) **Critical** criticality: conflict poses a major operational risk and must be resolved immediately

For example, selecting **yes** in the drop-down list of the Checklist (column F) when answering, *Can RH manage the O/S directly?* populates cell 6R in the Applied IT SOD Matrix associated with **O/S root access** (column R). The cell displays **M/C**, denoting a (**Medium**) **Critical** conflict. Instructions for remediating this conflict appear in columns T and U.

	A	B	C	D	P	Q	R	S	T	U
1					Recording	Recording	Recording	Recording		
2							Critical			
3							Y			
4			**Based on the job responsibilities and the application role/ responsibility setting, RH identifies the following SOD conflicted tasks:**		Perform Database Management Activities - DBA	Database - direct data change at the back-end	O/S root access	Perform Business User (BU) tasks (not read access) in the production application.		
5			**IT Task Description**		12	13	14	15		
6	Medium	Y	Develop Code	1			M/C		M/C 1. Verify that [DEVELOPER] who Develop Code is not [OSROOT] O/S root access.	M/C 1. Verify that [DEVELOPER] who Develop Code is not [OSROOT] O/S root access.
			Configure application	2						

Note that the Criticality Index used in the Applied IT SOD Matrix populates column A for the activity in column C. The index replicates the criticality values described above, with values appearing as **Low**, **Medium**, and **High**. In the example above, a **Medium** criticality value is given for the **Develop Code** test description.



	A	B	C	D	E	F	
1					Recording	Recording	Ver
2					Medium		
3					Y		
4			Based on the job responsibilities and the application role/ responsibility setting, RH identifies the following SOD conflicted tasks:		Developing Code	Configuring application	
5			IT Task Description		1	2	
6	Medium	Y	Develop Code	1			
			Configure application	2			

2.6 Users and Roles

The SOD Matrix template includes a **Role/User** spreadsheet to allow an analyst to identify and list application users and their corresponding roles.

Users listed in the Role/User list should align with the users and roles listed in the **Assets** spreadsheet (see §2.3).

Comparing the list of users and roles under the Role/User tab with those under the Assets tab allows the SOD analyst to build out the list of users and corresponding roles in the Role/User spreadsheet and to verify that all roles associated with the application are accounted for.

Red Hat

Separation of Duties [ANY-APPLICATION]

B6 | Developer

User Name	User Role	Last Updated
Bob Burridge	Developer	
Sally Smith	UAT	
Joy Jenkins	Manager	
Tony Tosca	Delivery Manager	
Larry Laughlin	Developer	

Generic SOD | Universal IT SOD Matrix | Assets | Checklist | Applied IT SOD Matrix | RoleUser | Analysis by User | Ass

3 SOD Analysis

The SOD analyst can perform a SOD analysis using either of two (or both) spreadsheets in the SOD Matrix template, as described below. Note that the role descriptions in both spreadsheets match the descriptions in the Applied IT SOD Matrix (see §2.2).

3.1 Analysis by User

The SOD Matrix template features an **Analysis by User** tab that allows an analyst to access a spreadsheet of user roles in a drop-down format to facilitate performing a SOD analysis. This method is preferred, as it allows quick reference at a glance of all users and their associated roles for any given application.

Red Hat

Separation of Duties [ANY-APPLICATION]

Security Warning Data connections have been disabled Options...

D7

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1				Recording	Recording	Verification	Verification	Verification	Authorization	Recording	Authorization	Recording	Recording	Recording	Recording	Recording	Recording
2				Medium													Critical
3																	
4				Y		0		0	0			0				0	Y
5				Developing Code	Configuring application	Performs unit test	Performs UAT	Code reviews	Approves changes - (code, configuration or patch)	Promote change to the production environment	Approve User Access	Application User Admin - access management (add/delete user)	Application Role Admin - role access management (add/delete entitlements within the role)	Configure batch job	Perform Database Management Activities - DBA	Database - direct data change at the back-end	O/S root access
6	Name	Expected	Code / Branch	1	2	3	4	5	6	7	8	9	10	11	12	13	14
7																	
8																	
9																	
10																	
11																	
12																	
13																	

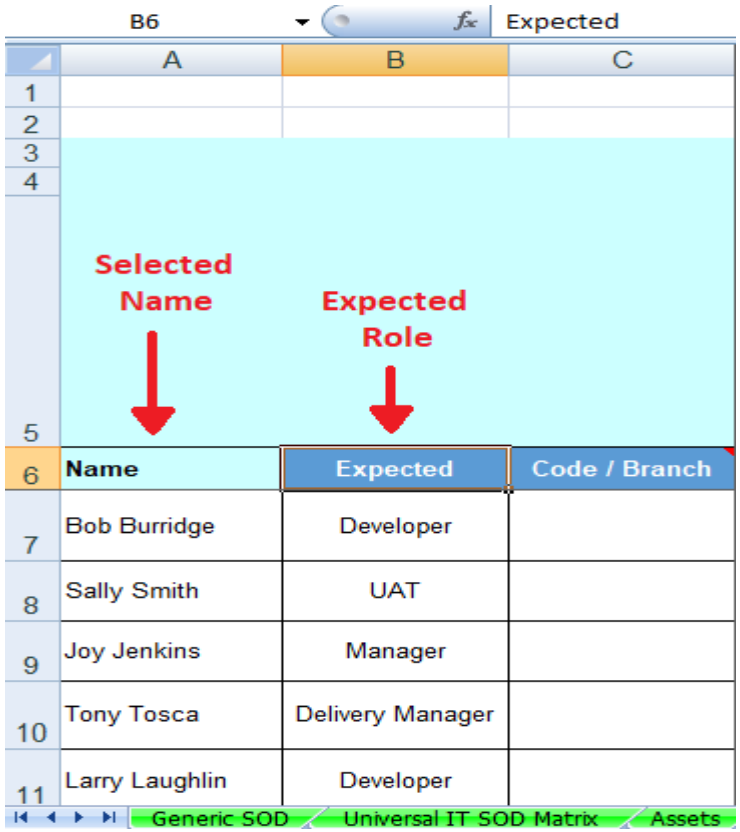
Generic SOD | Universal IT SOD Matrix | Assets | Checklist | Applied IT SOD Matrix | RoleUser | Analysis by User | Ass

Ready 80%

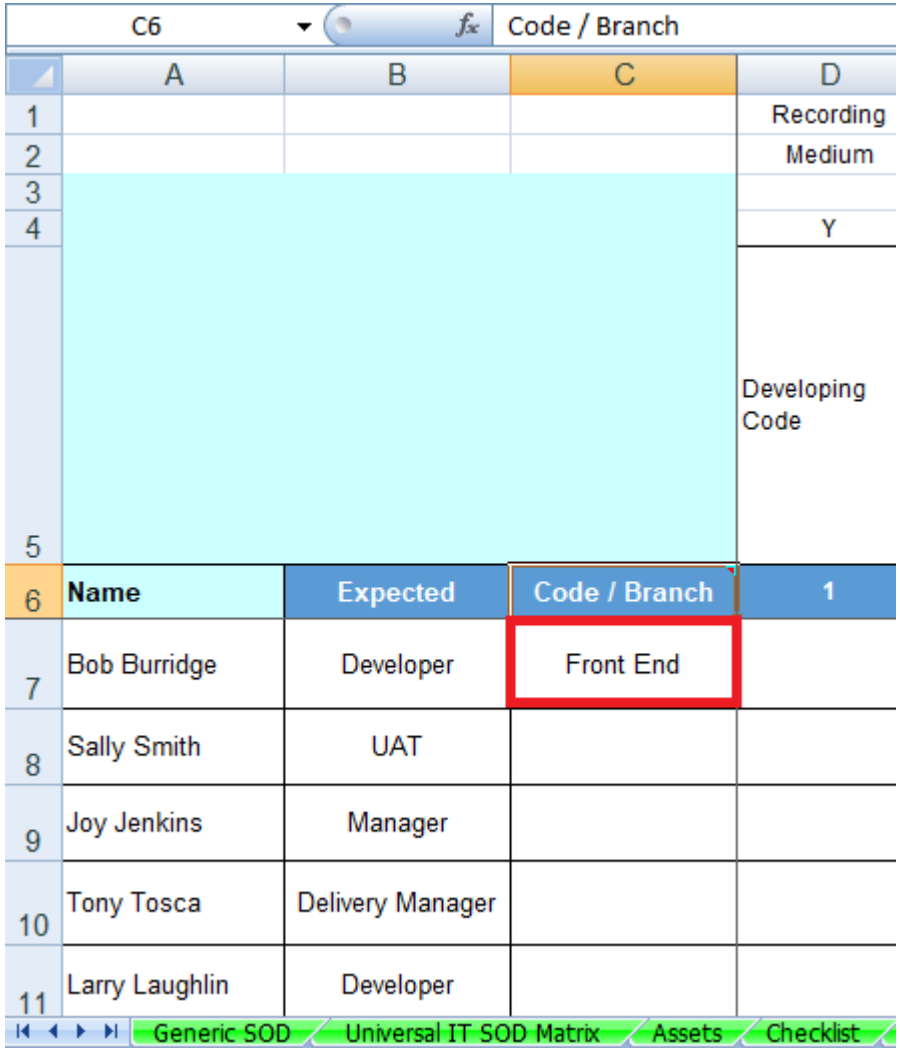
3.1.1 Populating Fields

Select the spreadsheet cells associated with the columns described below as follows:

1. In column A (**Name**), select the names of the application users from the drop-down list. Note that the list of users' names is extracted from those entered on the list under the Role/User tab.
2. With each name selected, an expected associated role auto-populates in column B (**Expected**).



3. In column C (**Code/Branch**), distinguish between identically named roles in column B by adding a qualifying description.



C6 | Code / Branch

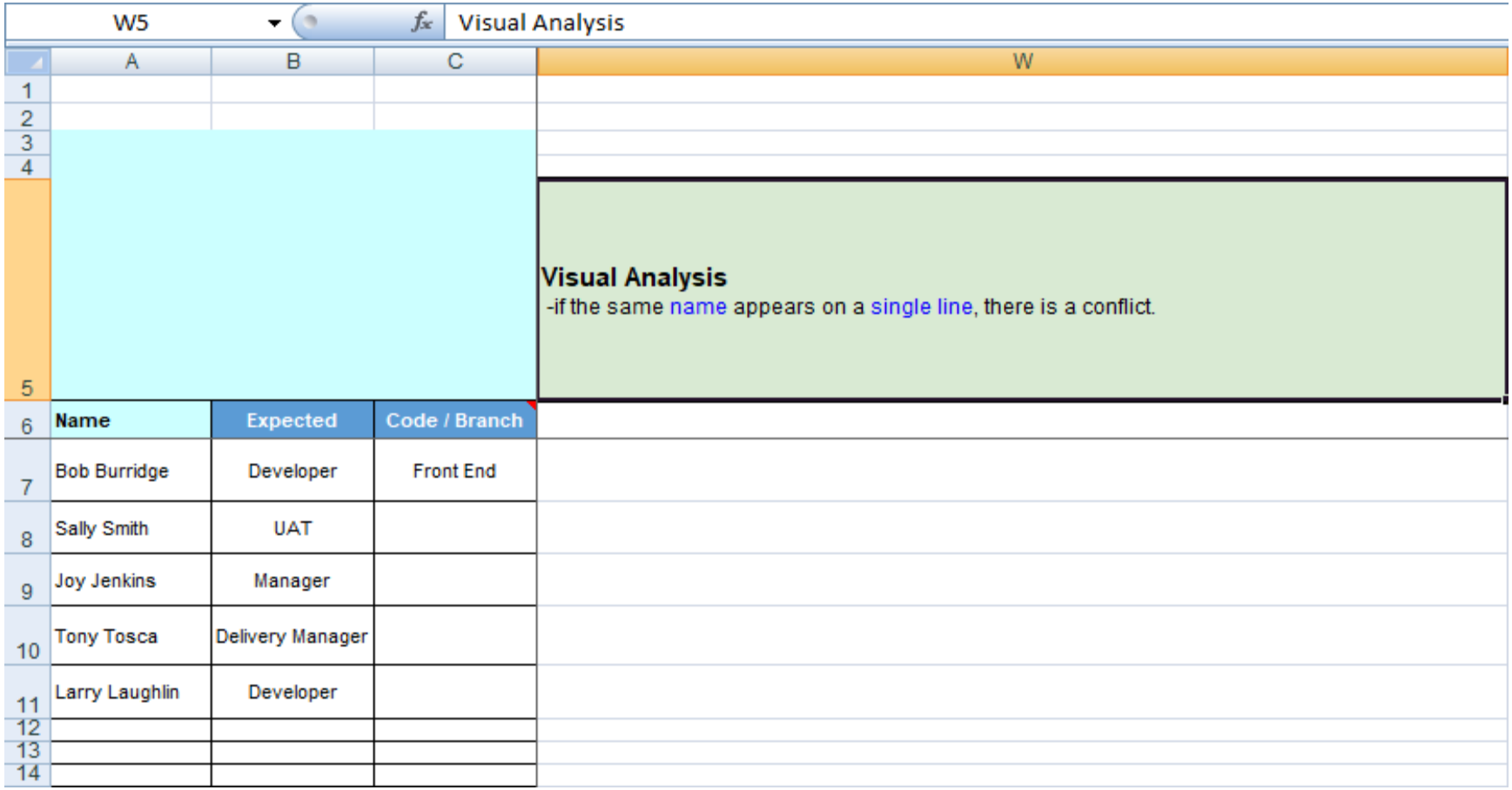
	A	B	C	D
1				Recording
2				Medium
3				
4				Y
5				Developing Code
6	**Name**	Expected	Code / Branch	1
7	Bob Burridge	Developer	Front End	
8	Sally Smith	UAT		
9	Joy Jenkins	Manager		
10	Tony Tosca	Delivery Manager		
11	Larry Laughlin	Developer		

Generic SOD | Universal IT SOD Matrix | Assets | Checklist

4. Additional identifying details about a named user's role can be selected as applicable from the drop-down lists in columns D - R, according to the role descriptions in row 5.

3.1.2 Conflicts

To the far right of the spreadsheet, in column W, is a **Visual Analysis** filter.



The filter automatically flags potential conflicts based on the analyst's selections in columns D - R. Conflicts are flagged when one or more selected roles potentially conflict with one or more other selected roles. If no conflicts are present, the Visual Analysis field will be empty.

Note: The Visual Analysis field will alert the analyst only to *potential* conflicts. It is incumbent on the analyst to determine whether the flagged role is in fact in conflict with one or more other roles.

In the following example, two potentially conflicting roles accrue to the user, each with an associated medium criticality (**M/C**) value (see §2.5).

Example

A7 | Bob Burridge

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1				Recording	Recording	Verification	Verification	Verification	Authorization	Recording	Authorization	Recording	Recording	Recording	Recording	Recording	Recording
2				Medium													Critical
3																	
4				Y		0		0	0			0				0	Y
5				Developing Code	Configuring application	Performs unit test	Performs UAT	Code reviews	Approves changes - (code, configuration or patch)	Promote change to the production environment	Approve User Access	Application User Admin - access management (add/delete user)	Application Role Admin - role access management (add/delete entitlements within the role)	Configure batch job	Perform Database Management Activities - DBA	Database - direct data change at the back-end	O/S root access
6	Name	Expected	Code / Branch	1	2	3	4	5	6	7	8	9	10	11	12	13	14
7	Bob Burridge	Developer	Front End	Bob Burridge			Bob Burridge		Bob Burridge								Bob Burridge
8	Sally Smith	UAT															
9	Joy Jenkins	Manager															
10	Tony Tosca	Delivery Manager															
11	Larry Laughlin	Developer															
12																	
13																	
14																	

Bob Burridge is identified by the roles visible in columns D, G, I, and Q.

Based on these roles, the Visual Analysis filter has generated alerts for two potential conflicts. The alerts direct the analyst to verify that:

- Bob Burridge the developer is not the same person who configures batch jobs.
- Bob Burridge the developer is not the same person who has operating system root access.

W7 | Conflict: Bob Burridge M/C Verify that [Bob Burridge] who Develops Code is not [Bob Burridge] who configures batch job.

	A	B	C	W	X	Y	
1							
2							
3							
4							
5				**Visual Analysis** -if the same name appears on a single line, there is a conflict.	**Manual Process / Final Analysis** a. Copy content of column (W) to column (X) using PASTE>VALUES b. Edit the column (X) analysis to ONLY display the VALID conflicts. c. Add Secondary Control in column (Z) if there is a conflict in column (X) OR c1. choose Y-"Risk Accepted by Red Hat" in column (Y)	Risk Acceptance	**Secondary/Comp**
6	**Name**	**Expected**	**Code / Branch**				Create text or link to S
7	Bob Burridge	Developer	Front End	Conflict: Bob Burridge M/C Verify that [Bob Burridge] who Develops Code is not [Bob Burridge] who configures batch job.			
8	Sally Smith	UAT		Conflict: Bob Burridge M/C Verify that [Bob Burridge] who Develops Code is not [Bob Burridge] with O/S root access.			
9	Joy Jenkins	Manager					
10	Tony Tosca	Delivery Manager					
11	Larry Laughlin	Developer					
12							
13							
14							

An analysis of the potential conflicts reveals that:

- Bob Burridge does not appear in the list of associates who perform batch jobs. The first alert then is not applicable.
- The Bob Burridge who develops code IS the Bob Burridge who has operating system root access. The second alert then points to an actual conflict.

Resolve the analysis as follows:

1. Manually copy the content from the Visual Analysis cell in column W and paste it into the **Manual Process/Final Analysis** cell in column X by right-clicking and selecting Paste special > Paste **values** only.
2. Edit the content in the Manual Process/Final Analysis cell by deleting the alert that is not applicable.

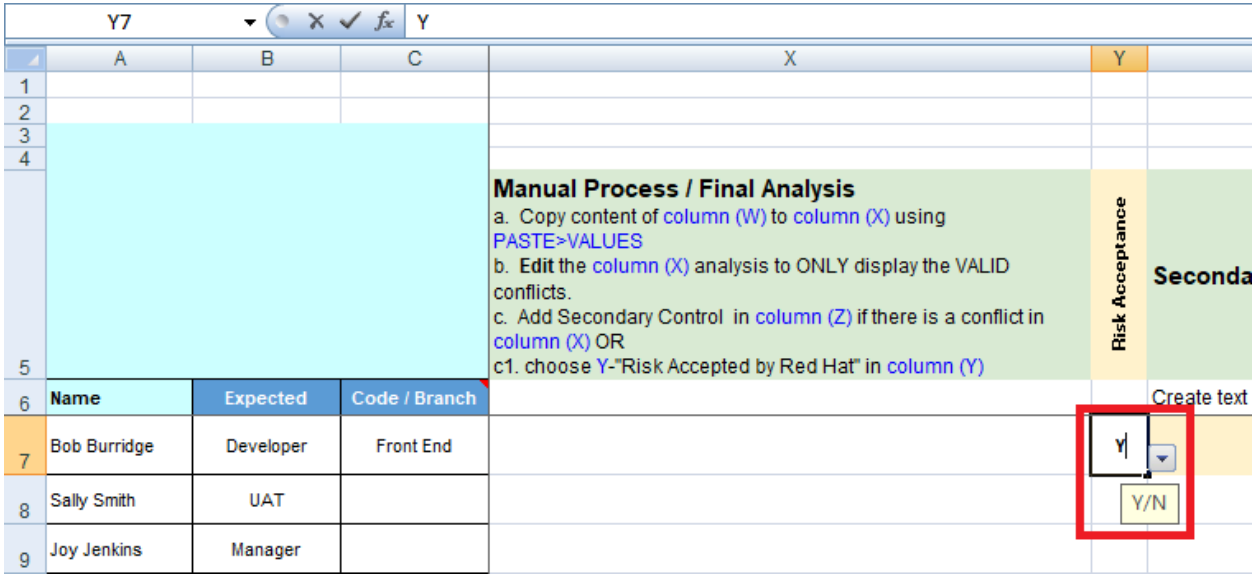
   Note: The Manual Process/Final Analysis cell appears in beige highlight to denote that the Visual Analysis cell contains content and that further analysis is required. The highlight is triggered when a **Risk Acceptance** determination is made that a risk is unacceptable (see step 4, following). This color-coded logic appears throughout the spreadsheet wherever an additional action must be taken. Once appropriate action is taken, the cell highlight disappears.

3. Determine whether it is acceptable for Bob Burridge to have operating system root access.

   ### Discussion

   Ask whether the code Bob is developing is intended for the operating system root. If it is, then root access is probably permissible as it is part of Bob's defined role. In this case, Bob's code would require review by another qualified associate to verify that the code is in fact developed specifically for the operating system root, ruling out any potential conflict. If, however, Bob's code is developed for a purpose other than for the operating system root, then a determination must be made about whether Bob's access to the operating system root is necessary based on Bob's defined role(s) and whether his access represents a significant risk.

4. Column Y provides a cell with a drop-down for quickly assigning a **Risk Acceptance** determination based on the evaluation performed in step 3. Is the risk acceptable? Select **Y**, **N**, or **?** (TBD).



5. In the cell in column Z, enter any criteria that represent a **Secondary/Compensating Control**. In this example, a compensating control could be e.g. a requirement that Bob Burridge retain access to the operating system root, but that this access can be conferred only after Bob's code is vetted by management.

Z7 | All code that is moved into the O/S is management approved.

	A	B	C	X	Y	Z	AA	AB
1								
2								
3								
4								
5				**Manual Process / Final Analysis** a. Copy content of column (W) to column (X) using PASTE>VALUES b. **Edit** the column (X) analysis to ONLY display the VALID conflicts. c. Add Secondary Control in column (Z) if there is a conflict in column (X) OR c1. choose Y-"Risk Accepted by Red Hat" in column (Y)	**Risk Acceptance**	**Secondary/Compensating Control**	**Remediation Action:** Roles are Redefined	**Notation** - This may be the link to a Acceptance Doc
6	**Name**	**Expected**	**Code / Branch**			Create text or link to Secondary Control / Desk Procedure		
7	Bob Burridge	Developer	Front End			All code that is moved into the O/S is management approved.		
8	Sally Smith	UAT						
9	Joy Jenkins	Manager						
10	Tony Tosca	Delivery Manager						
11	Larry Laughlin	Developer						
12								
13								
14								

6. If a Secondary/Compensating Control is not warranted, enter in the cell in column AA any **Remediating Action(s)**, e.g. limiting Bob's role and his corresponding access privileges and/or reassigning Bob's role to another user.

AA7 | Reassign Bob's O/S root access to Larry Laughlin.

	A	B	C	Y	Z	AA	AB	AC	AD	AE	AF
1											
2											
3											
4											
5				Risk Acceptance	**Secondary/Compensating Control**	**Remediation Action:** Roles are Redefined	**Notation** - This may be the link to a specific Risk Acceptance Doc				
6	**Name**	**Expected**	**Code / Branch**		Create text or link to Secondary Control / Desk Procedure						
7	Bob Burridge	Developer	Front End			Reassign Bob's O/S root access to Larry Laughlin.					
8	Sally Smith	UAT									
9	Joy Jenkins	Manager									
10	Tony Tosca	Delivery Manager									
11	Larry Laughlin	Developer									
12											
13											
14											

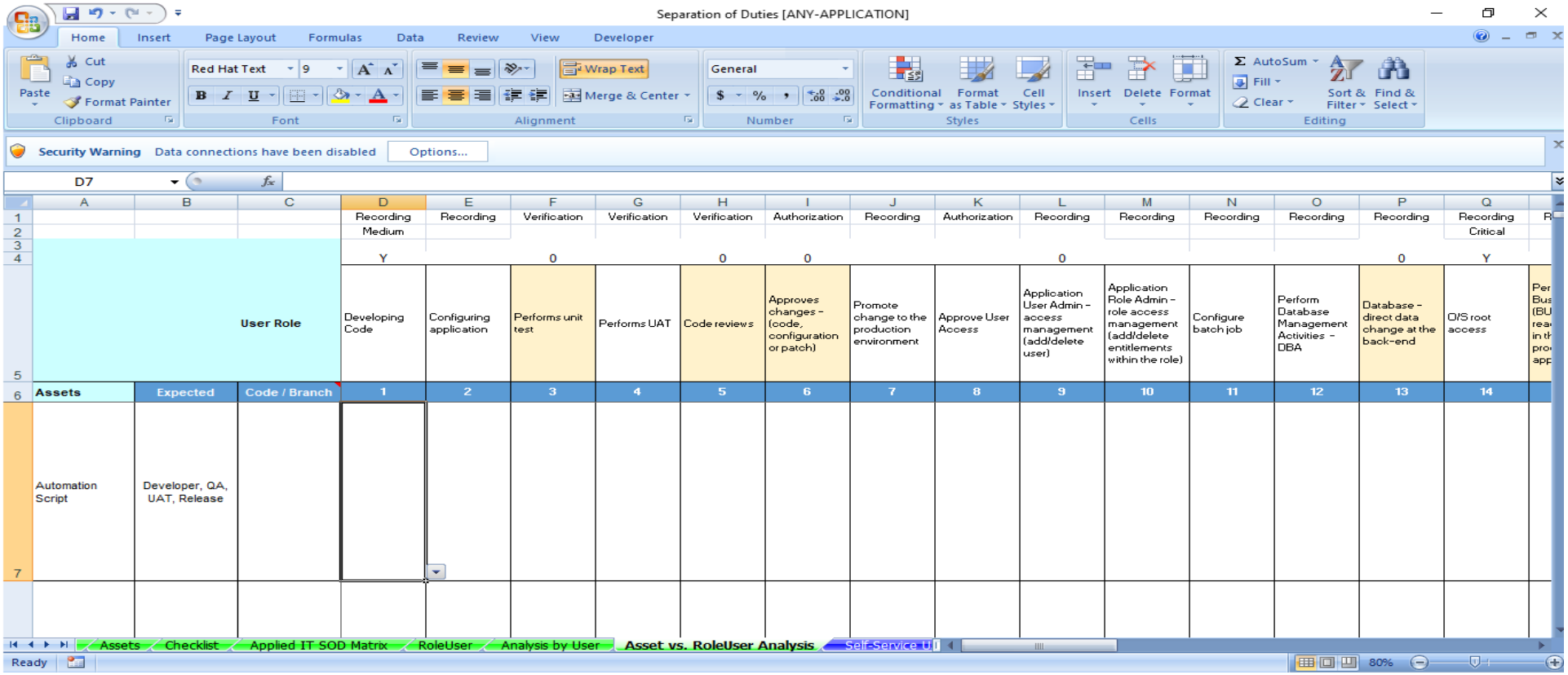
7. Add any newly defined users from step 6 to the Role/User spreadsheet under the **Role/User** tab.
8. Column AB provides a **Notation** cell that can be used to provide links to risk acceptance or other supporting documentation.
9. Repeat steps 1-8 for each user listed in column A.

If, in the example above, a determination is made that Bob Burridge's access privileges constitute an acceptable risk (by selecting **Y** in column Y; see step 4), then the color-keyed action alerts disappear from the cells in columns Z, AA, and AB and no further action must be taken.

Completion of the steps above addresses identified conflicts and constitutes an action plan that allows the analyst to show an auditor that the business unit has a controlled process in place compliant with SOD principles.

3.2 Asset versus Role/User Analysis

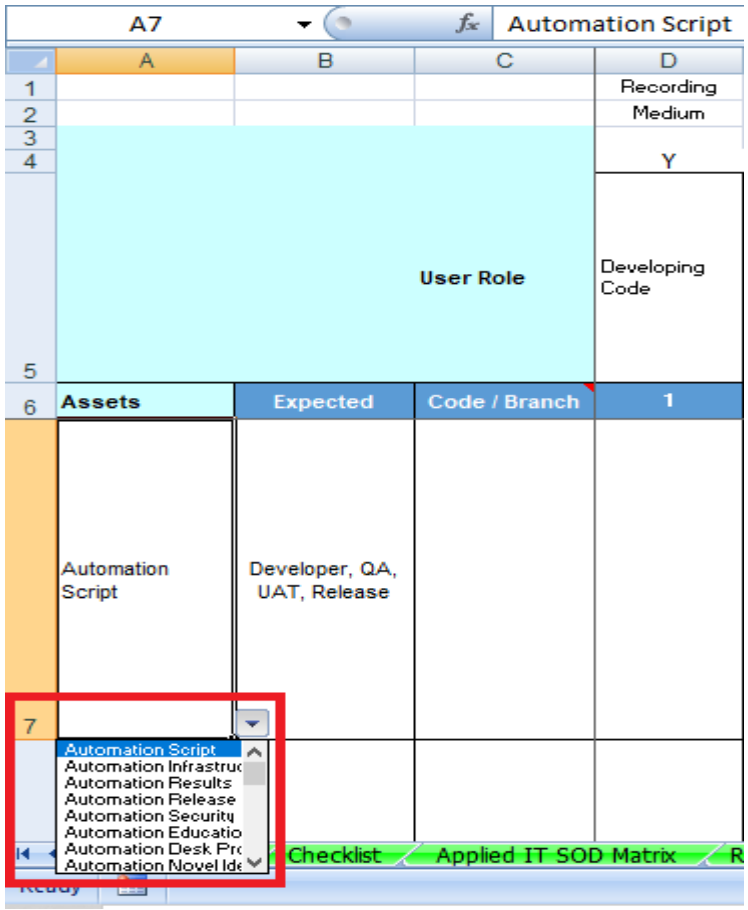
As an alternative to performing an **Analysis by User**, an analyst can perform a SOD analysis by filling in a spreadsheet under the **Asset vs Role/User Analysis** tab. Analysis is performed by user name or by role, following each line item. Final results using this analysis tool will match results when performing an Analysis by User.



3.2.1 Populating Fields

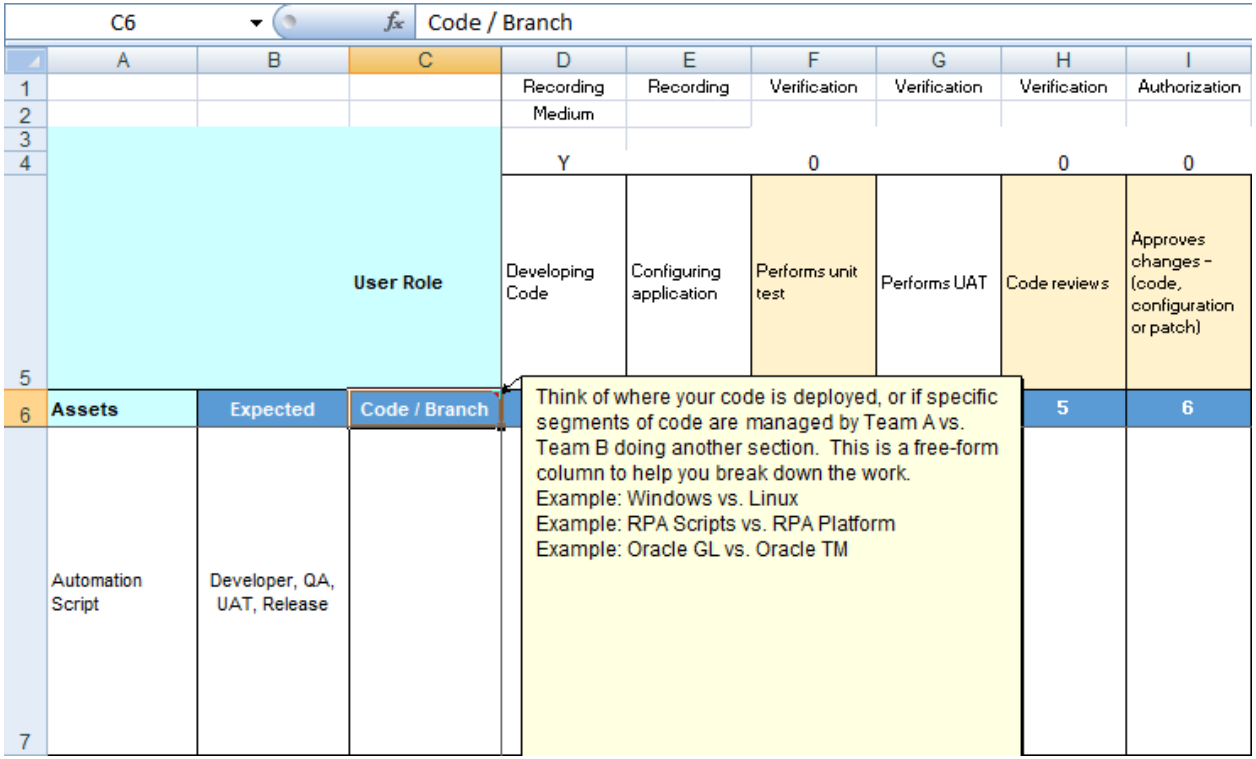
Select the spreadsheet cells associated with the columns described below as follows:

1. Column A (**Assets**), features a drop-down that replicates the assets listed under the Assets tab (see §2.3). Select the asset to be analyzed from the list.

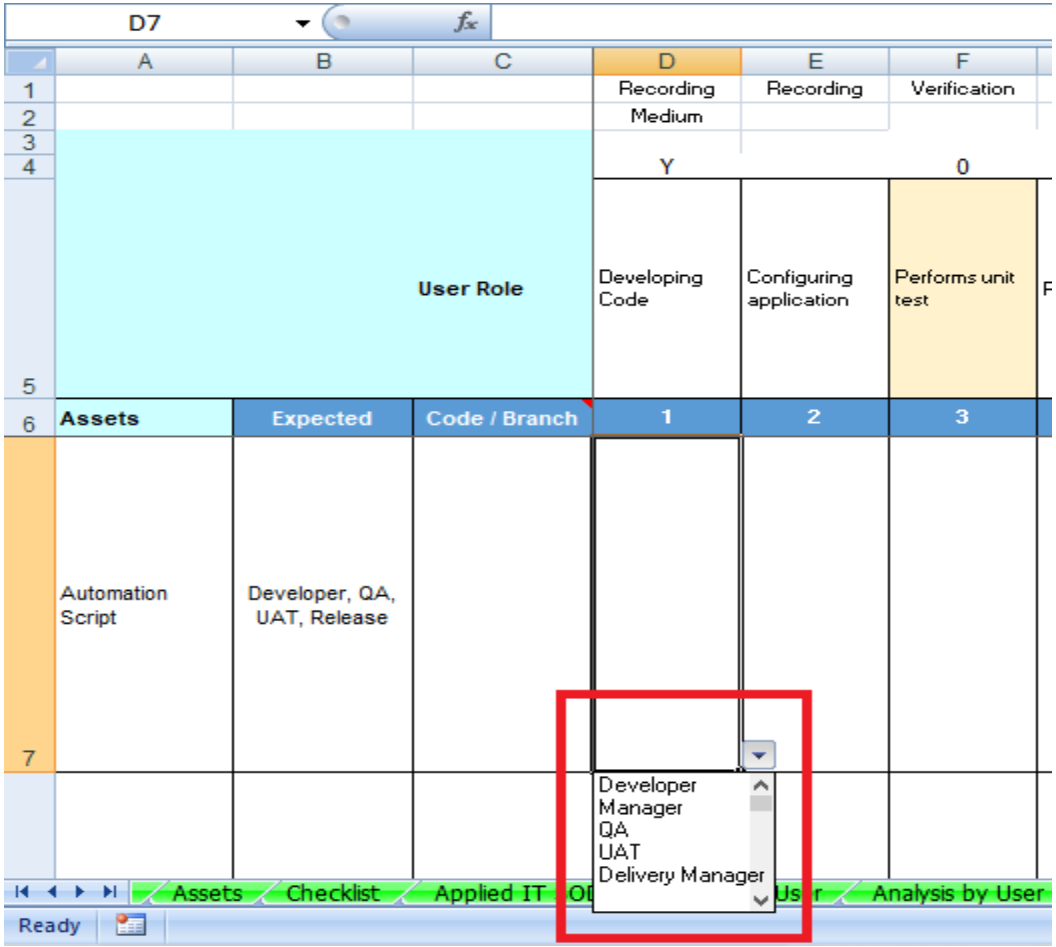


Note: Each asset is correlated with an expected user role. Expected roles, based on the asset selected, are derived from column C of the Assets spreadsheet (**Who does the work?**). Roles populate automatically in column B of the Asset vs Role/User Analysis spreadsheet (**Expected**).

2. Modify column B as appropriate.
3. Column C (**Code/Branch**) features a drop-down that allows an analyst to perform a SOD analysis using either a user's name or a user's role. Open cells beginning on line 7 are free-form and allow an analyst to note anything relevant to branch management, etc. Use of the cells is optional.



4. Additional identifying details about a listed asset can be selected as applicable from the drop-down lists in columns D - R, according to the role descriptions in row 5.



Note: the criteria that appear in the drop-down lists in columns D - R change depending on the type of analysis selected in step 3.

3.2.2 Conflicts

Conflicts when using the Asset vs Role/User Analysis spreadsheet are identified and resolved in the same manner as when using the Analysis by User spreadsheet. For a complete discussion on resolving these conflicts, see §3.1.2 (all).

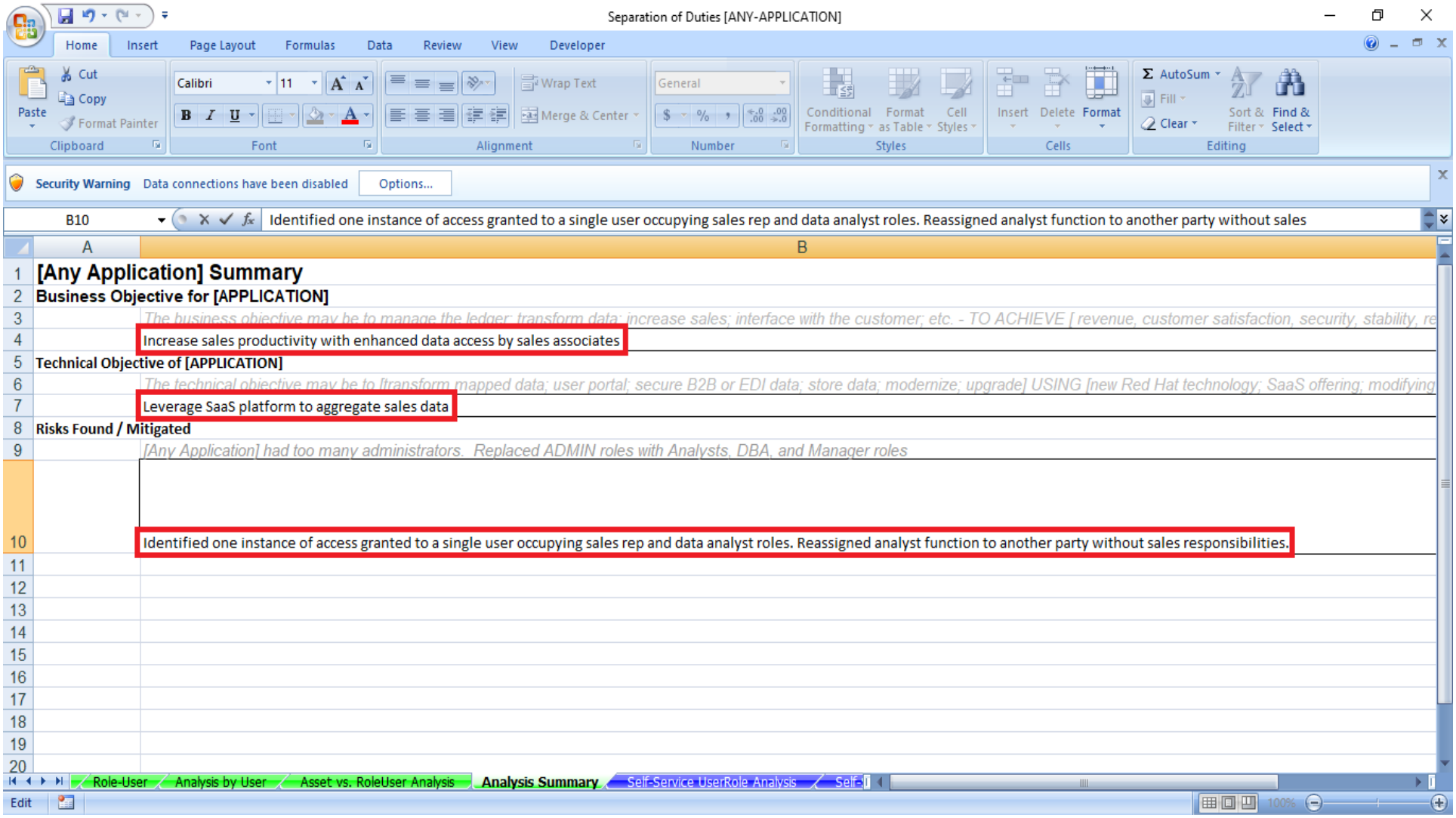
4 Remediation

For each of the tools described above, the object is the same; SOD conflicts can be methodically resolved using either tool. However, an analyst should be mindful that any remediation indicated in step 6 of the Discussion above must be concluded before proceeding with the audit. Failure to do so will ensure an actionable result during the audit.

A list of Secondary/Compensating Controls for a potential conflict is acceptable going into the audit, as such controls indicate an awareness of the conflict and concomitant deployment of a solution.

5 Analysis Summary

The SOD Matrix includes an **Analysis Summary** spreadsheet that an analyst can use to create a brief summary description of the business objective for the application, a technical objective, and any risks identified and remediated. Use of the summary is optional.



6 Revision History

Version Number	Nature of Change	Author/Editor	Date Approved
1.0	Initial version	Adam Hardesty	July 16, 2021