RECIPE FOR SUCCESS

CAJPA

2017 CONFERENCE

Who’s Policing the IT Police?

RECIPE FOR SUCCESS

SEPTEMBER 12-15, 2017
SOUTH LAKE TAHOE, CA

Who’s Policing the IT Police?

Rick Krepelka, Chief Operations Officer
Golden State Risk Management Authority

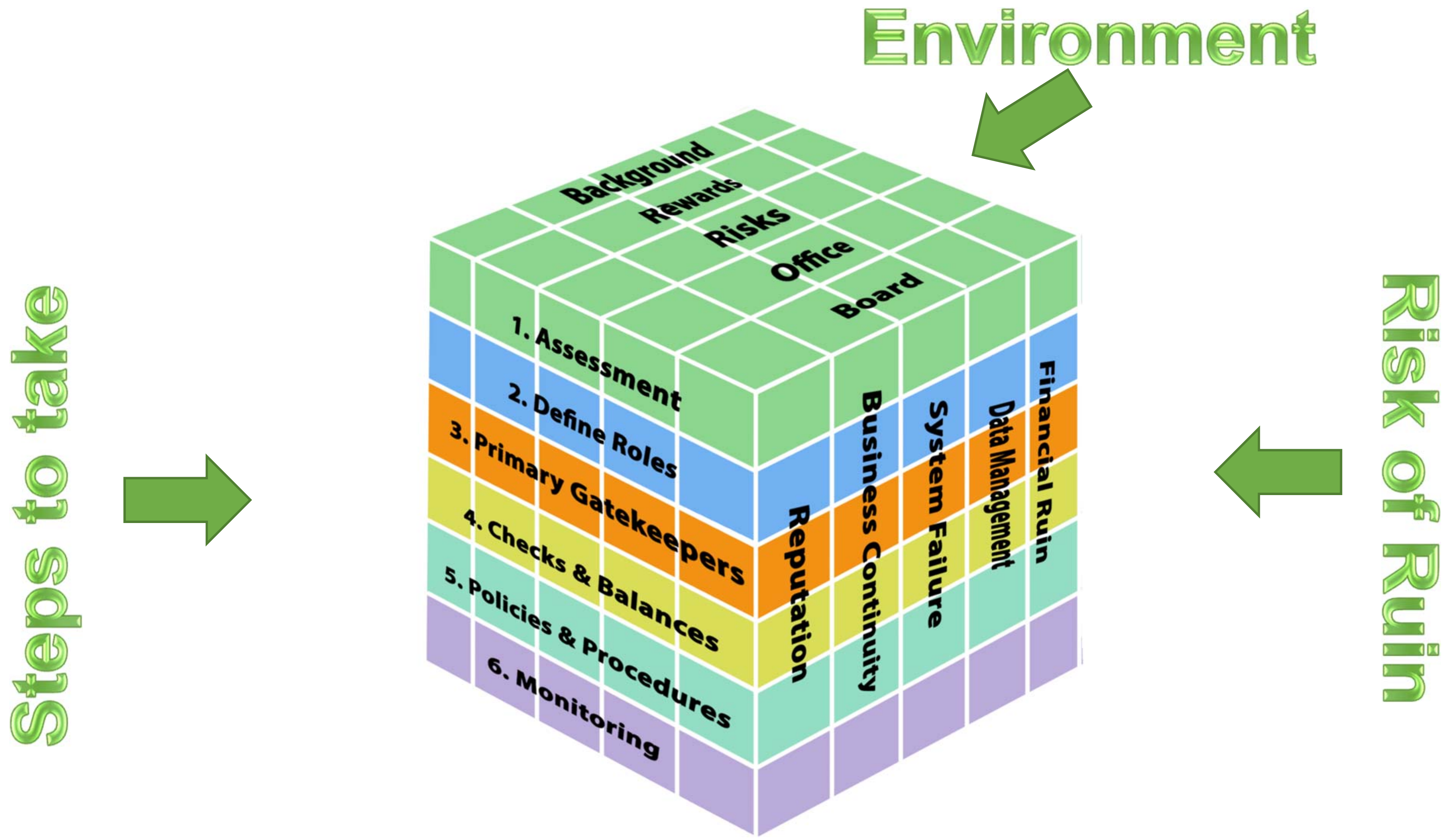
Tommy Le, IT/IS Manager
Washington Schools Risk Management Pool (WSRMP)

Ritesh Sharma, Manager, Finance & Accounting
Bickmore

How Did This Happen?!

- Prior to computer technology, “access” was managed with physical locks and keys.
- Advent of technology -> The keys became technology-based so IT became the gatekeepers.
- Technology permeates the workplace and the IT gatekeepers suddenly are very powerful…and it’s very scary.

KLS IT Police Framework



What Systems?

Financial

- Banking
- Accounting
- Investment
- Claims

What Systems? (cont.)

Data

- Underwriting
- HR/Employee benefits
- Contact management/CRM
- Claims

What Systems? (cont.)

Operations

- Network
- Computer systems/devices
- Portals
- Intranet

What Systems? (cont.)

Other

- Company website
- Worksheets & documents

What’s At Risk?

- Financial Ruin:
  - Theft from internal or external agents
  - Errors by employees
- Data Management:
  - Data breach
  - Compromised information

What’s At Risk? (cont.)

- Operations Management:
  - Critical systems failure
  - Business continuity
- Any of the Above:
  - Publicity nightmare
  - Loss of faith

What To Do?

1. Identify systems and data repositories that require protection.
2. Define roles for the various parties requiring access.
3. Address the issue of “primary gatekeeper(s)” of each system.

What To Do? (cont.)

4. Develop checks and balances to reduce risk.
    - Preventive controls
    - Compensating controls
5. Develop policies and procedures to manage and enforce the roles.
6. Conduct periodic review and evaluation; Engage external auditor or reviewer to evaluate systems and processes.
    - Detective controls

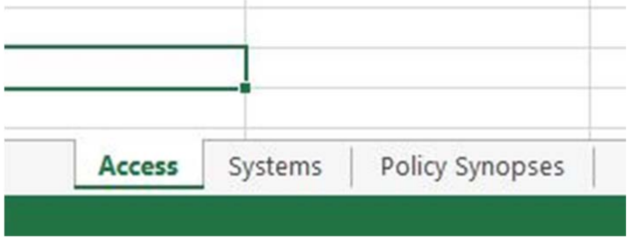
An Example…

Formalizing a System of Security …

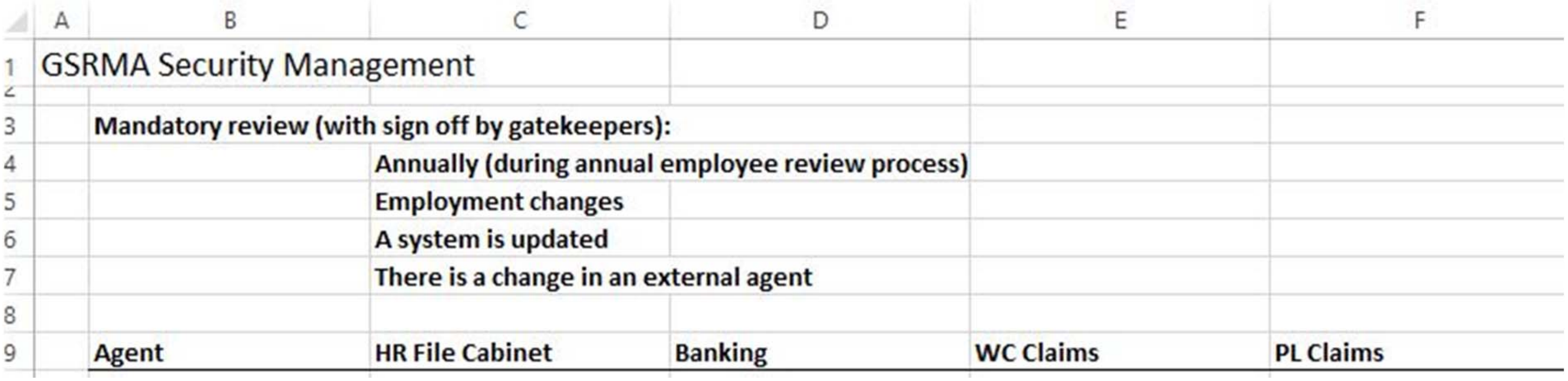
A simple case study

Example (Slide 1 of 6)

System of Security - > Excel

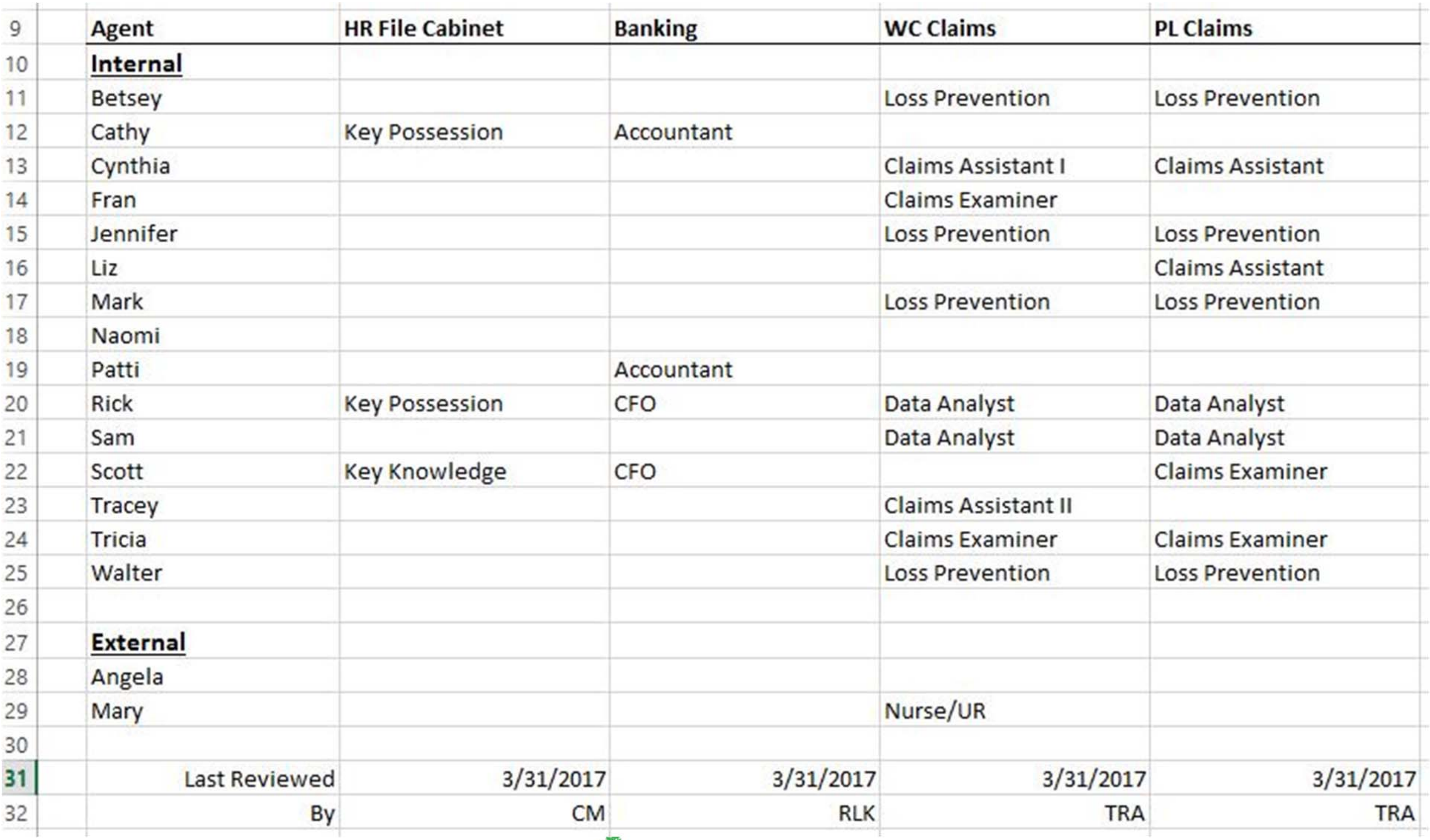


Example (Slide 2 of 6)



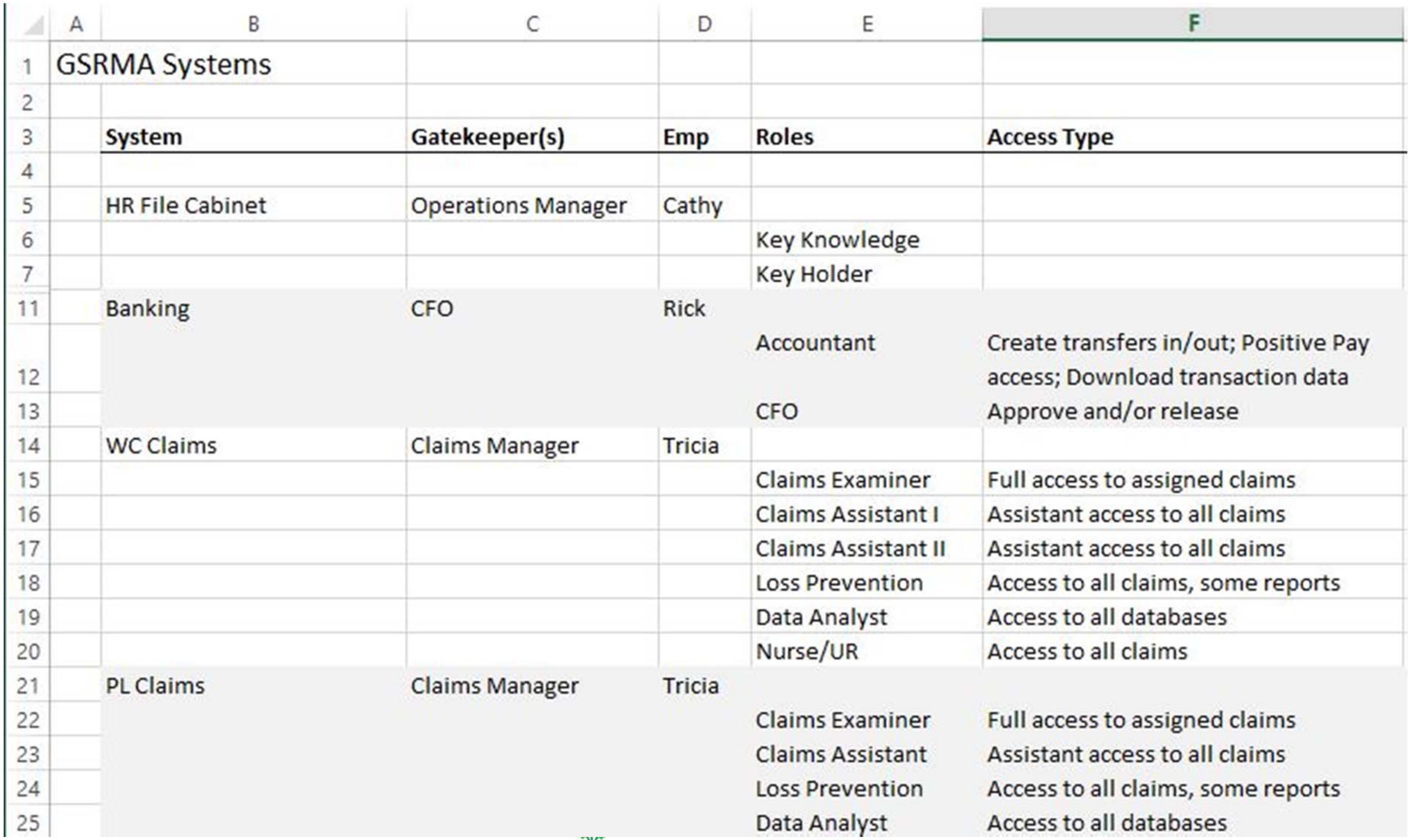
	A	B	C	D	E	F
1	GSRMA Security Management					
2						
3		Mandatory review (with sign off by gatekeepers):				
4			Annually (during annual employee review process)			
5			Employment changes			
6			A system is updated			
7			There is a change in an external agent			
8						
9		Agent	HR File Cabinet	Banking	WC Claims	PL Claims

Example (Slide 3 of 6)



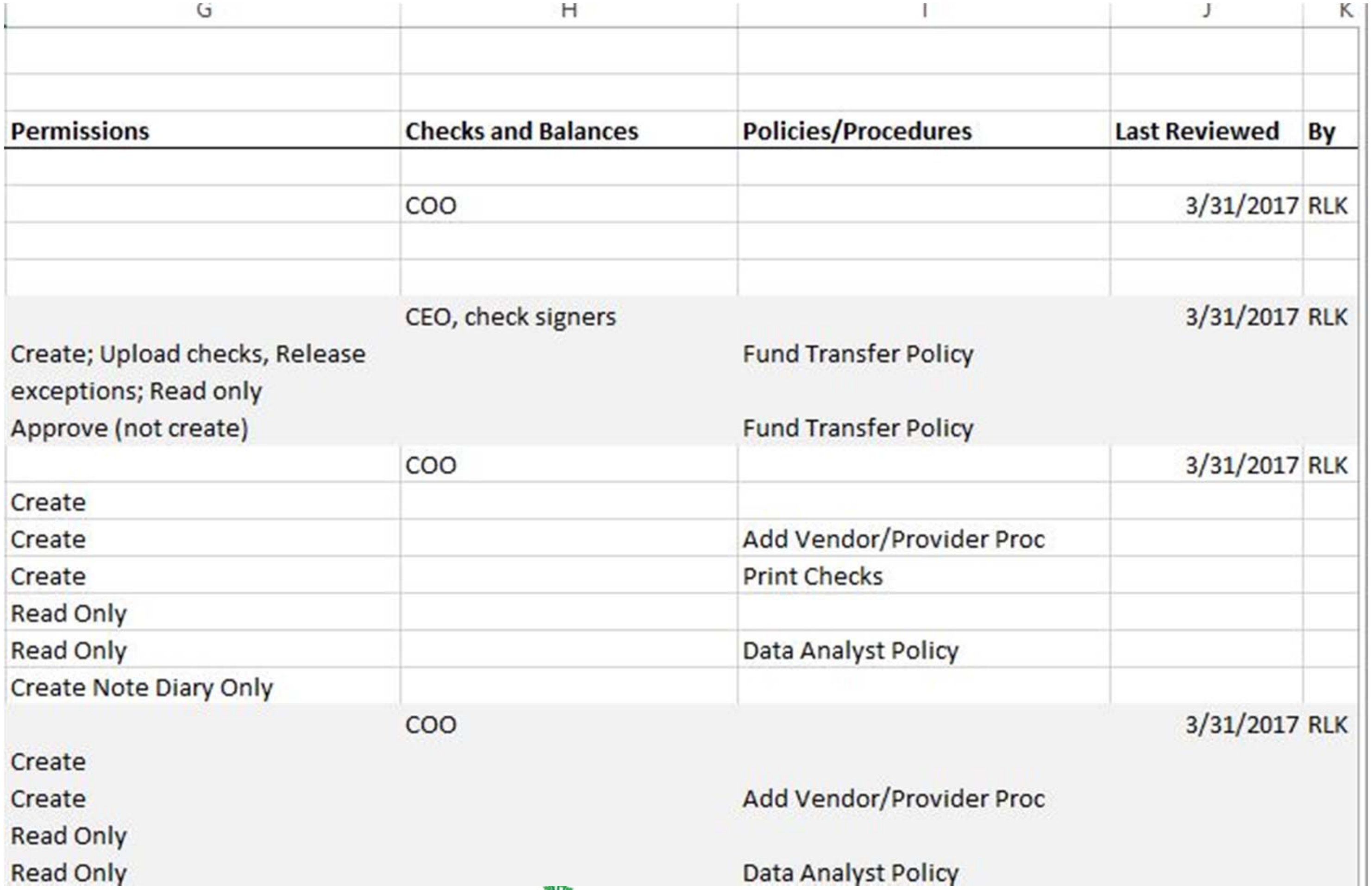
9	Agent	HR File Cabinet	Banking	WC Claims	PL Claims
10	**Internal**				
11	Betsey			Loss Prevention	Loss Prevention
12	Cathy	Key Possession	Accountant		
13	Cynthia			Claims Assistant I	Claims Assistant
14	Fran			Claims Examiner	
15	Jennifer			Loss Prevention	Loss Prevention
16	Liz				Claims Assistant
17	Mark			Loss Prevention	Loss Prevention
18	Naomi				
19	Patti		Accountant		
20	Rick	Key Possession	CFO	Data Analyst	Data Analyst
21	Sam			Data Analyst	Data Analyst
22	Scott	Key Knowledge	CFO		Claims Examiner
23	Tracey			Claims Assistant II	
24	Tricia			Claims Examiner	Claims Examiner
25	Walter			Loss Prevention	Loss Prevention
26					
27	**External**				
28	Angela				
29	Mary			Nurse/UR	
30					
31	Last Reviewed	3/31/2017	3/31/2017	3/31/2017	3/31/2017
32	By	CM	RLK	TRA	TRA

Example (Slide 4 of 6)



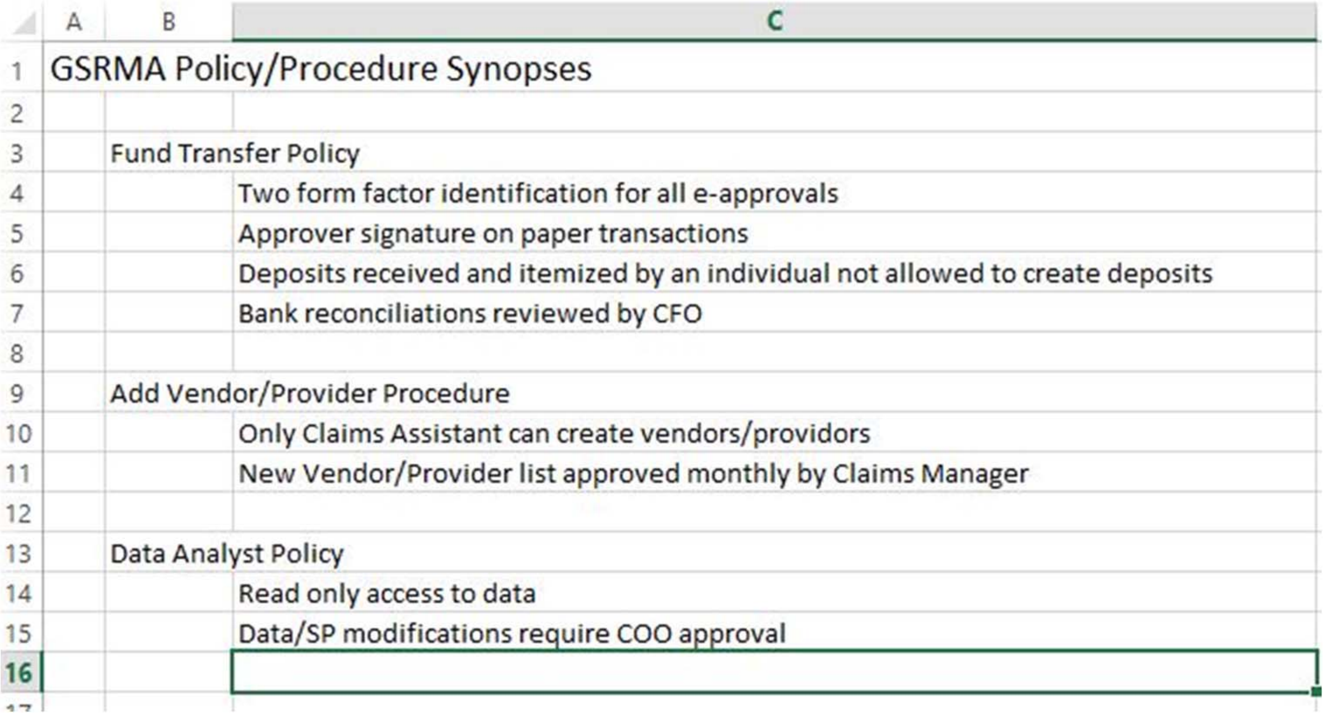
	A	B	C	D	E	F
1	GSRMA Systems					
2						
3		**System**	**Gatekeeper(s)**	**Emp**	**Roles**	**Access Type**
4						
5		HR File Cabinet	Operations Manager	Cathy		
6					Key Knowledge	
7					Key Holder	
11		Banking	CFO	Rick		
12					Accountant	Create transfers in/out; Positive Pay access; Download transaction data
13					CFO	Approve and/or release
14		WC Claims	Claims Manager	Tricia		
15					Claims Examiner	Full access to assigned claims
16					Claims Assistant I	Assistant access to all claims
17					Claims Assistant II	Assistant access to all claims
18					Loss Prevention	Access to all claims, some reports
19					Data Analyst	Access to all databases
20					Nurse/UR	Access to all claims
21		PL Claims	Claims Manager	Tricia		
22					Claims Examiner	Full access to assigned claims
23					Claims Assistant	Assistant access to all claims
24					Loss Prevention	Access to all claims, some reports
25					Data Analyst	Access to all databases

Example (Slide 5 of 6)



G	H	I	J	K
Permissions	**Checks and Balances**	**Policies/Procedures**	**Last Reviewed**	**By**
	COO		3/31/2017	RLK
	CEO, check signers		3/31/2017	RLK
Create; Upload checks, Release exceptions; Read only		Fund Transfer Policy		
Approve (not create)		Fund Transfer Policy		
	COO		3/31/2017	RLK
Create				
Create		Add Vendor/Provider Proc		
Create		Print Checks		
Read Only				
Read Only		Data Analyst Policy		
Create Note Diary Only				
	COO		3/31/2017	RLK
Create				
Create		Add Vendor/Provider Proc		
Read Only				
Read Only		Data Analyst Policy		

Example (Slide 6 of 6)



	A	B	C
1	GSRMA Policy/Procedure Synopses		
2			
3		Fund Transfer Policy	
4			Two form factor identification for all e-approvals
5			Approver signature on paper transactions
6			Deposits received and itemized by an individual not allowed to create deposits
7			Bank reconciliations reviewed by CFO
8			
9		Add Vendor/Provider Procedure	
10			Only Claims Assistant can create vendors/providors
11			New Vendor/Provider list approved monthly by Claims Manager
12			
13		Data Analyst Policy	
14			Read only access to data
15			Data/SP modifications require COO approval
16			

“Where Do I Start?”

- NIST Special Publication 800-14
  Generally Accepted Principles and Practices for Securing Information Technology Systems
- Can be done in bite-sized pieces
- Get buy-in from the top
- Share the load ASAP

Scenario #1

IT gives full claims system access to the claims examiner. Claims examiner is an experienced user, claims manager is not. Claims manager was not aware that access was given to claims examiner.

Scenario #2

Remote access or making data or systems available on the cloud can improve efficiency. However, the benefits can be greatly diminished if security is too restrictive.

Scenario #3

Accounting manager receives an email from the board president. It includes an invoice from a vendor and instructions to wire payment to the vendor immediately.

Who’s Policing The IT Police?
Questions or Comments

GOLDEN STATE RISK MANAGEMENT AUTHORITY	Rick Krepelka
WS RMP WASHINGTON SCHOOLS RISK MANAGEMENT POOL	Tommy Le
Bickmore	Ritesh Sharma