

# NextGen GRC

## A Case Study

Andy Clauson, GRC Analyst, Cyber Security

Kaiser Permanente

Wednesday, October 2, 2013



Trust in, and value from, information systems

San Francisco Chapter



2013 Fall Conference – “Sail to Success”

*CRISC*

*CGEIT*

*CISM*

*CISA*

# Case Study Contents

- Background and challenges
- Our take on NextGen GRC
- Case study #1: DLP integration
- Case study #2: findings
- Lessons learned
- Q & A

# Kaiser Permanente: Key Facts

- Nation's largest not-for-profit health plan
- Over 9 million members
- 37 hospitals
- 618 medical offices and other facilities
- More than 175,000 employees
- 17,157 physicians; 49,034 nurses
- \$50.6 billion operating revenue
- Largest Private Electronic Medical Records Program
- More than 19 million visits to mobile-optimized kp.org



**2012: Five star rating from CMS for Medicare plans in California.**



# Regulatory Environment


- PCI
- HIPAA
- SOX
- State regulations
- Many others
- Gaining in complexity
- Relatively rapid changes
- Compounded by Kaiser Permanente's highly federated organizational structure



# Security Environment

- Thousands of applications
- Tens of thousands of servers
- Hundreds of thousands of endpoints
- Hundreds of thousands of internal users
- Millions of external (web, etc) users
- Standard array of emerging challenges  
(mobile, IP enabled medical devices, etc)

# GRC Org Structure: Convergence within IT

- 
- Multiple IT security and compliance functions reorganized into a Technology Risk Office
  - Shift in focus from a department's silo (eg compliance or security) to the common goal of risk management
  - Mandate to share information and processes
  - *Long term good idea that causes short term uncertainty in business process and therefore technology need*

# Summary



# What NextGen GRC is

## Classic GRC Approach

Primarily for Mapped Control Set -> Assessments -> Findings -> Remediation workstream, and compliance reporting

Do All At Once / a single implementation

Attempt to make a single software accomplish data aggregation, transactional needs, history, assessment, security, etc etc

Architect for full automation of an often pie in the sky future state business process. Assume the auditor can be replaced with computer logic.

## Next Gen GRC

Productivity for G or R or C personnel ; compliance and other reporting as a natural byproduct

Go for small wins (add value where you can with eye on bigger picture)

Recognize you need a full suite of tools, at a minimum a RDBMS for your big data, a transactional / workflow engine, sophisticated reporting capability-- and lots integration potential to smash value ceilings.

Architect for simplicity, flexibility and future growth. Automate only mature operational processes. Do not attempt to replace the CISA / professional human judgment. Instead aim to add productivity.

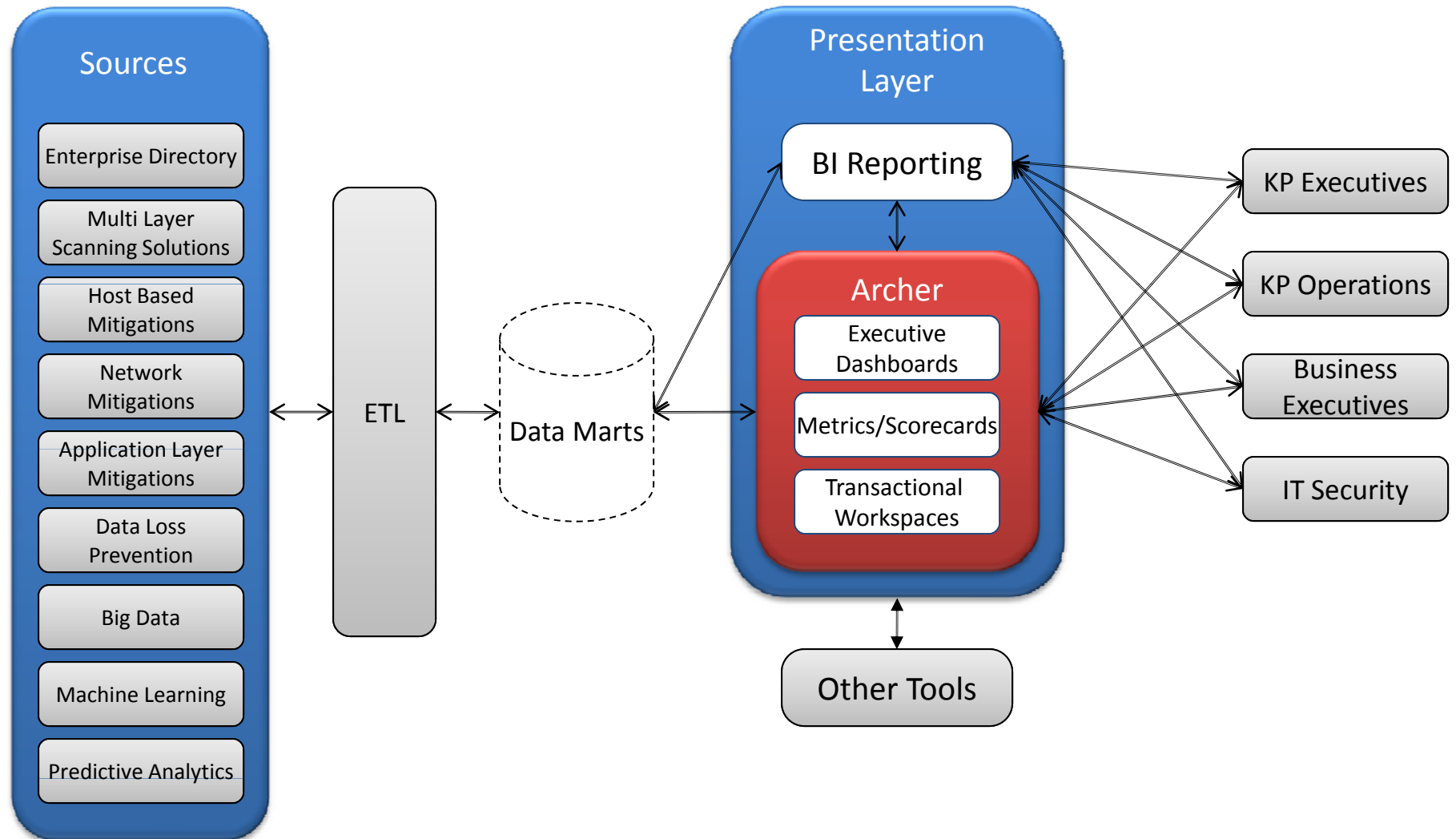


# What NextGen GRC is NOT

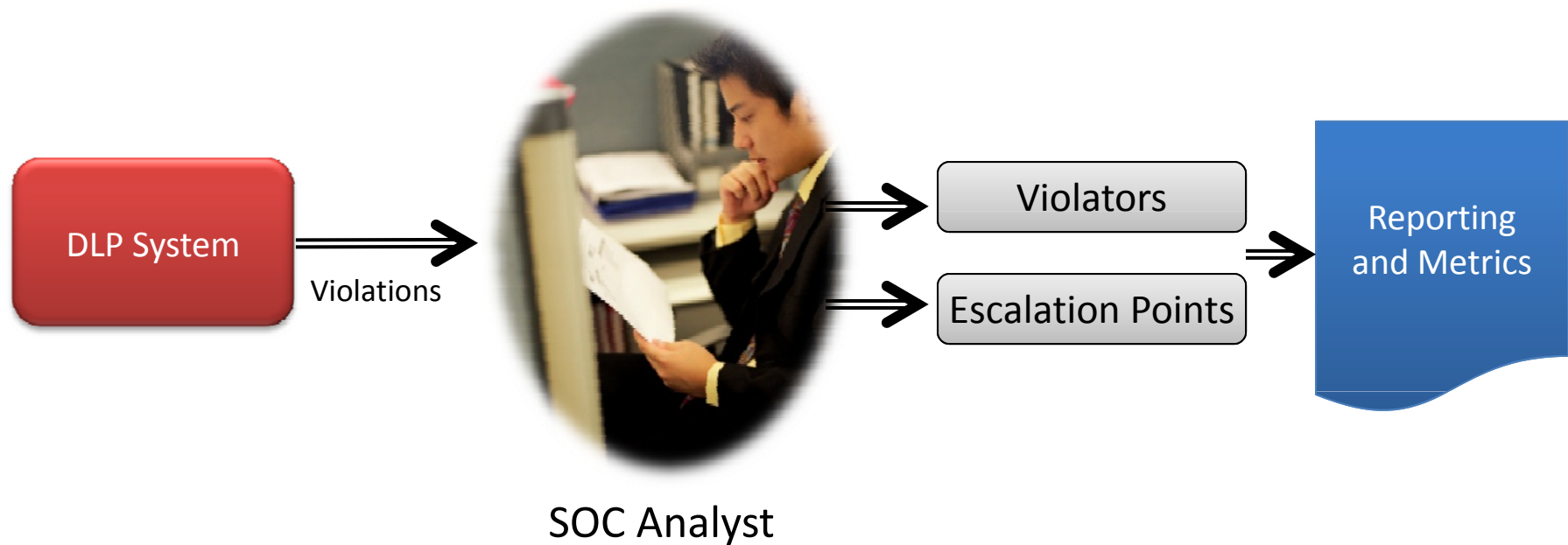
- Totally unstructured
- Make up requirements as you go
- Without testing (must have a test script populated with expected outcomes)
- Without project management



# Sample NextGen GRC Architecture



# Simple Example: DLP Integration



# Issues and options

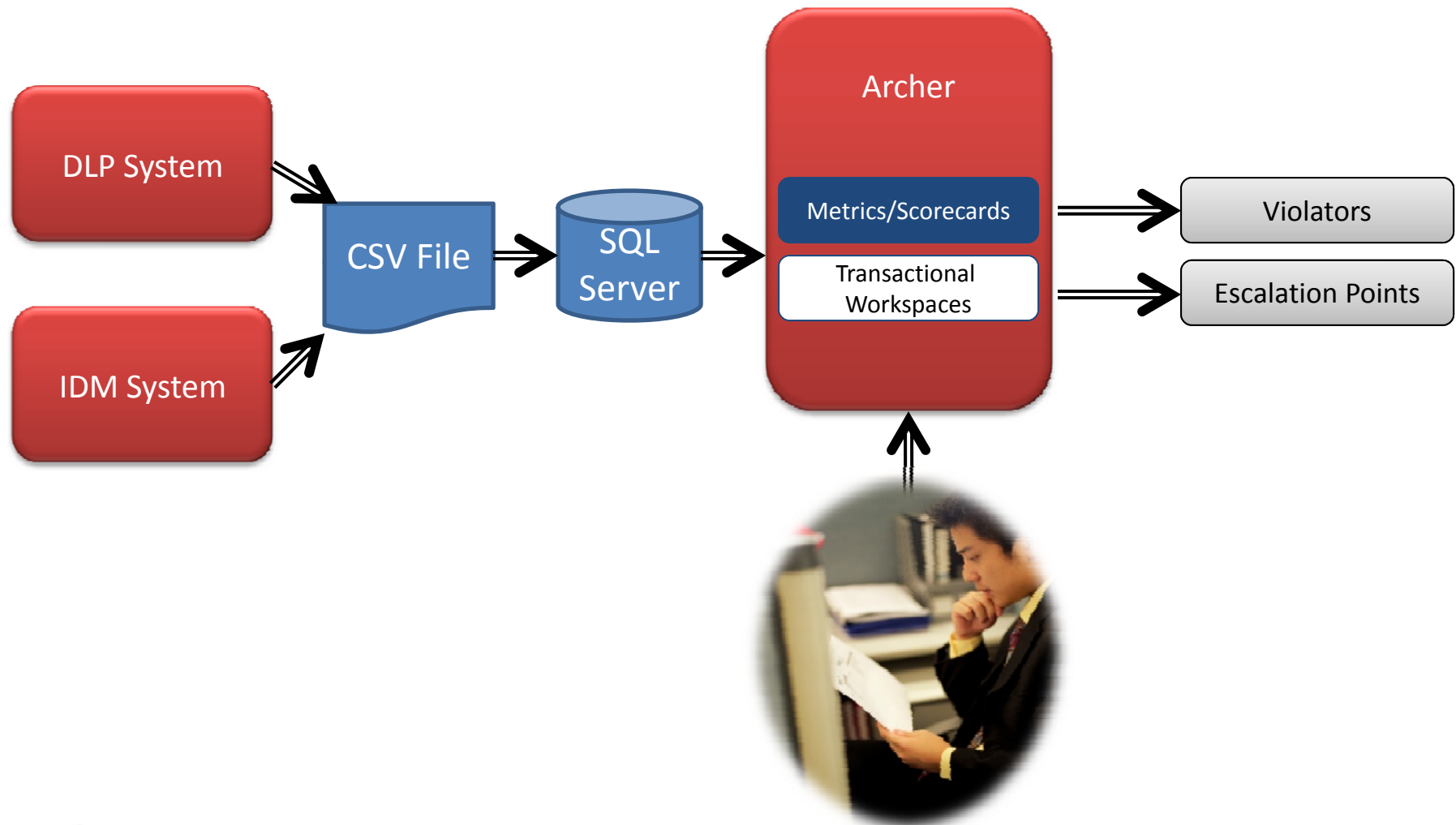
- DLP API may be nascent
- Process may be still ramping up
- Requirements for what we would need in the future may lead to speculation and many possible future outcomes

- 
- Option A: Wait and discuss (analysis paralysis)
  - Option B: Chip off and implement the pieces that add value now

# Implementation

- Break the total project into bite-sized pieces to score incremental gains.
- Smash the value ceiling in our DLP and GRC system by writing a custom script to export and transform the data
- Enable flow of metrics data between departments by leveraging common infrastructure
- Bring only the data that's needed for transactional work into GRC, leave the rest in an external data store
- Subsequent phases to do the email and other enforcement actions

# Implementation Overview



# Example 2: Processing findings in a risk-oriented environment



# Issues and options

- Risk rating, mapping , etc needs to be injected
- Multiple moving targets makes process automation a challenge
- Option A: Wait and discuss (analysis paralysis)
- Option B: Chip off and implement the pieces that add value now

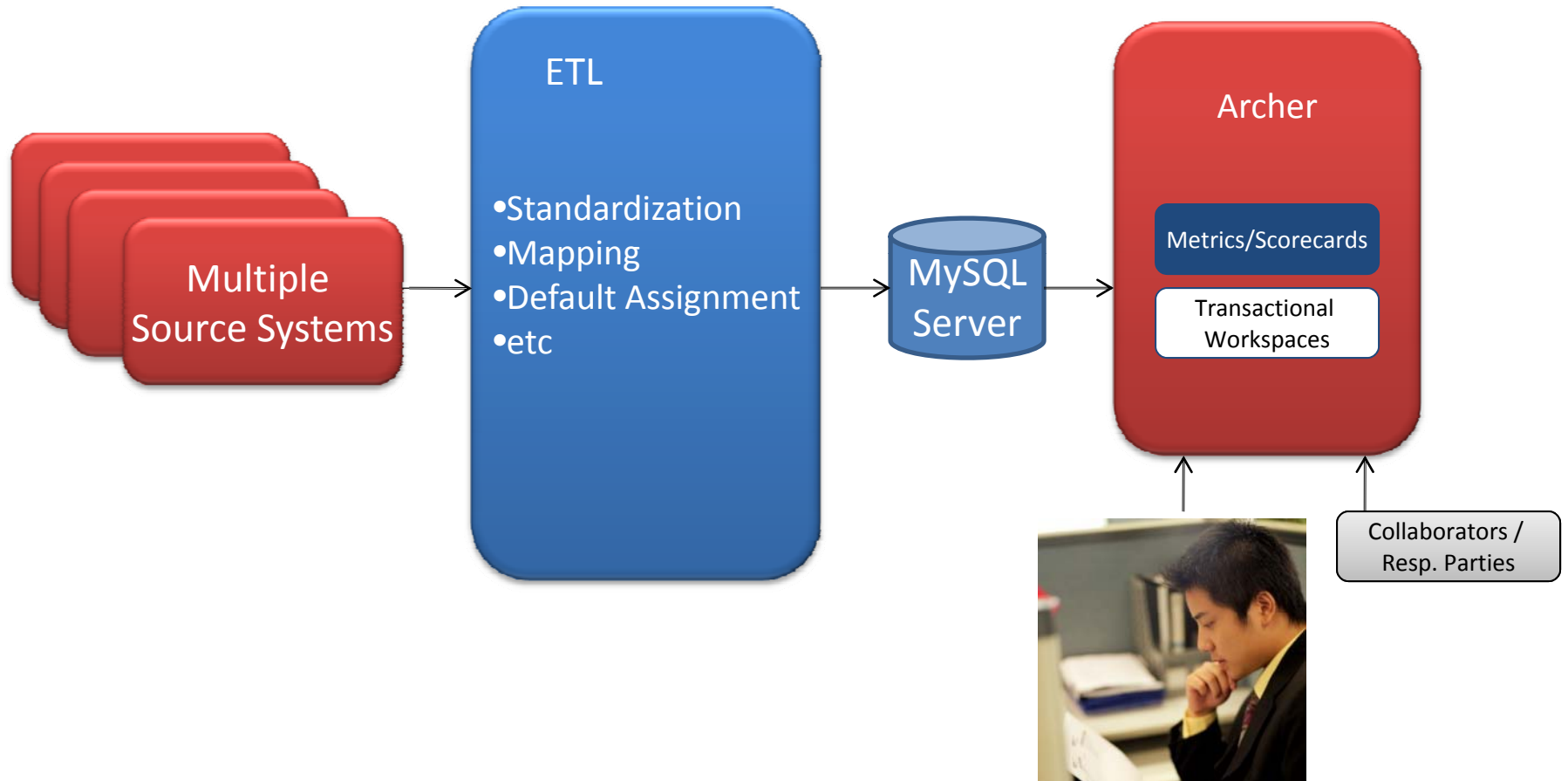


# Implementation




- ETL (extract transform load) to gather, systematically classify and prioritize findings
- Use GRC system to provide a common workspace and basis for reporting

# Implementation



# Lessons learned

- 
- Providing value early is the only way to go
  - Do not jettison discipline in the rush to provide value
  - Flexibility and simplicity go hand in hand
  - Use software for its strength

# Q & A

