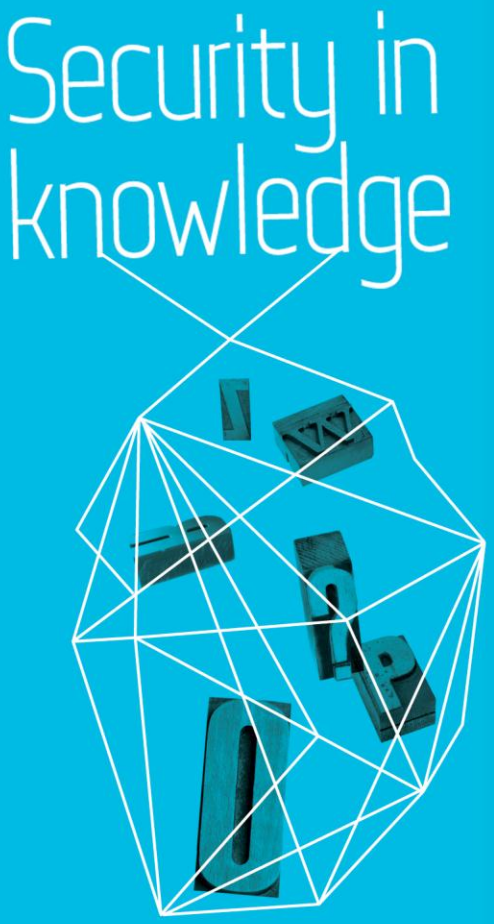
MANAGING DAILY SECURITY OPERATIONS WITH LEAN AND KANBAN



Gene Kim
IT Revolution Press

Branden R. Williams
HireBranden.com

Session ID: END-W22

Session Classification: Intermediate

AGENDA AND OBJECTIVES

- Discuss Lean & Applicability
- Reveal Challenges with the Volume of Work
- Discuss the Three Ways
- Show Transformation Phases
- Drink and be Merry

HOW IS AN IT/IS PERSON'S DAY PRIORITIZED TODAY?

1: THE BIGGEST FIRE

2: THE LOUDEST EXECUTIVE

WHERE DOES THIS LEAD US?

- To the hamster wheel of pain and suffering!

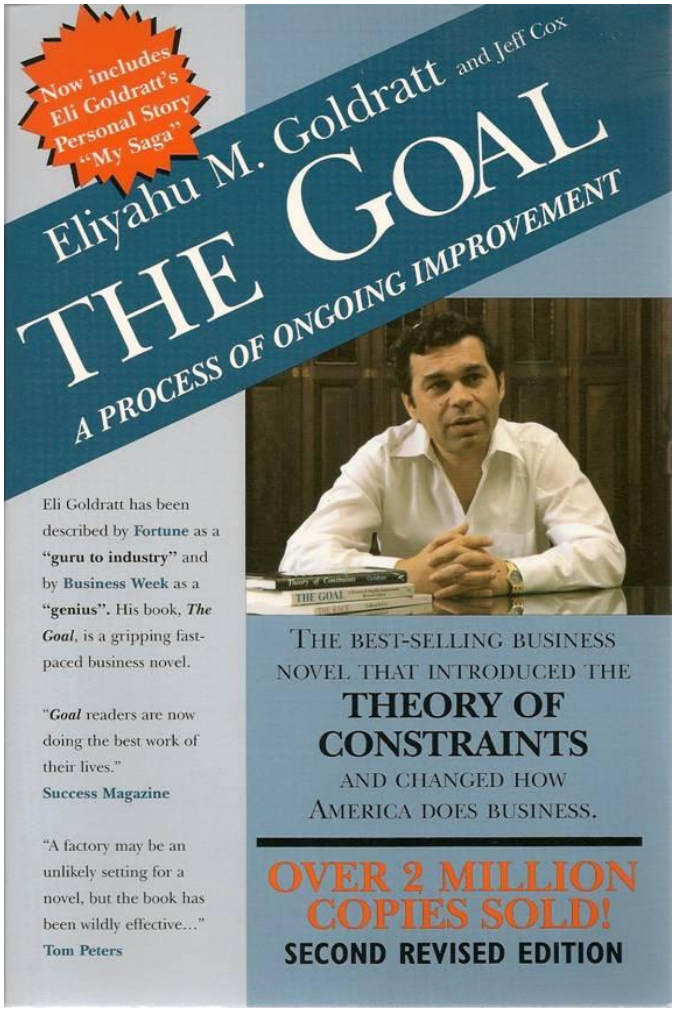
The Familiar Problem (Scrub for non-dupes)

- We get dumped on by everyone
- Our work is always late
- We sometimes make promises that we can’t deliver on
- We defer work that we shouldn’t
- No one takes ‘no’ for an answer
- We act before understanding the business
- Business is dissatisfied with our work

THERE MUST BE A BETTER WAY…

THE GOAL, DR. ELIYAHU M. GOLDRATT

- Who here is an MBA?
- You've probably read this!
- Introduces Theory of Constraints



IT SECURITY IS AN ELECTRONIC FACTORY

- Concepts that drive physical factories can drive IT/IS work
  - Lean production in factories can teach us quite a bit about systems and types of work
  - Physical or digital, the concepts apply universally
- We have inputs, WIP, and outputs
  - Some of our inputs and outputs may not be tangible (unless printed)
- What is WIP?
  - Work In Process, or work that is incomplete
  - It is neither raw materials nor a finished product
  - Ties up input resources and prevents useful outputs from flowing through
  - It's the gunk in the IT/IS machine!

WHAT IS LEAN?

- Lean is a system that does two things:
  - Reduce waste
  - Improve throughput
- Common analogies:
  - Manufacturing (plants)
  - Supply chain
- Key differentiator:
  - PULL system
  - VISUALIZED work

THE FIRST WAY: SYSTEMS THINKING (L TO R)

- Understand the flow of work
- Always seek to increase flow
- Never unconsciously pass defects downstream
- Never allow local optimization to cause global degradation
- Achieve profound understanding of the system

WHAT IS WORK?

- Inputs:
  - Dev project reviews
  - Prep for upcoming audits
  - Deploy security technologies
  - Fix audit findings
  - Migrate from virtual to cloud
  - Preventive projects to elevate constrain
- WIP:
  - Unfinished projects
  - Code changes prior to deploy
  - Uncommitted changes

WHAT IS WORK? (CONTINUED)

- Outputs
  - Completed projects
  - Services running
  - Audits complete
  - Completed projects
  - Happy customers

EXAMPLE: A TYPICAL TODO LIST

But wait....
THERE'S
MORE!! (duh)

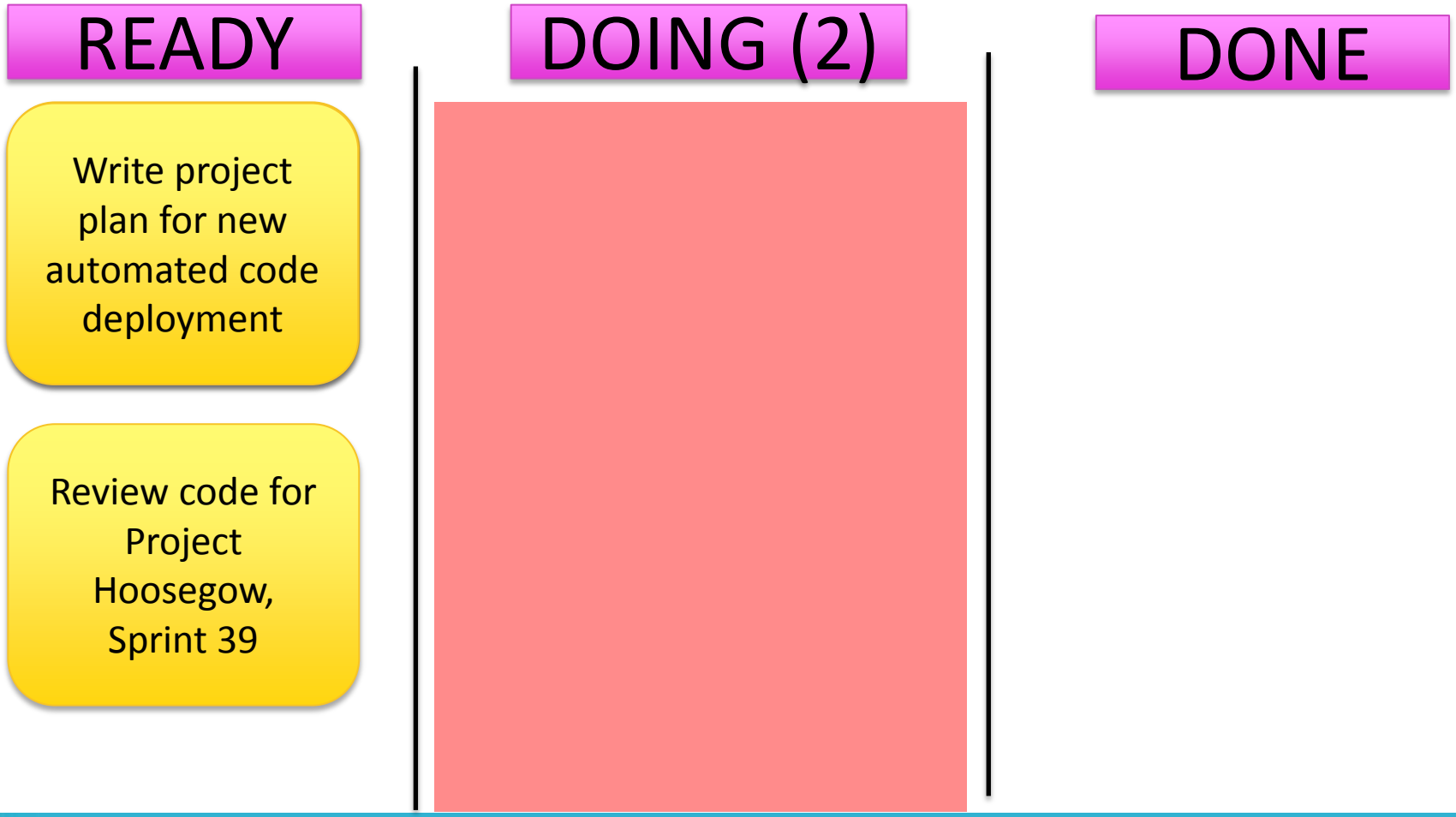
EXAMPLE: A LONGER TYPICAL TODO LIST

- Reach out to new internal auditor
- Think about unified control strategy for compliance (3rd year on TODO list)
- Create appointment with developer, asking to stop avoiding input validation (who is his manager?)
- Find out who owns server TWX-44-9113: is port 9050 really supposed to be open? (TOR?)
- Respond to angry email from Marketing director: privacy regulations aren't optional (!!)
- Email Sarah: please take me off the physical security alert list
- Read that report from external auditor: can't TL;DR any more

KANBAN

- What is it, and why does it work?
  - Created by Taiichi Ohno (Toyota)
  - Scheduling board for lean production
  - Good: Visualizes work in a system
  - Better: Visualizes work FLOW THROUGH a system
- Outcomes: WORK GETS DONE!
  - Work takes less time to complete (i.e., reduced cycle time, on time!)
  - Better tracking of effort and costs
  - Find recurring work that we can automate
  - Find work where there's too much time 'waiting' or 'in queue'
  - Business gets what they need, when they need it
  - Infosec becomes viewed as a reliable partner

SAMPLE KANBAN PROCESS W/WIP LIMITS



WHAT WORK IS REALLY MOST IMPORTANT?

- Top line goals of top executives exist for a reason
  - Does your work align to those goals?
  - Does it help those executives meet those goals?
  - If not, WHY ARE YOU DOING IT?
- Understand where controls exist in the business
  - As the keeper of the IT controls, are you responsible for catching everything?
  - What other controls exist in the business that you can leverage to avoid putting work into the system?
  - Or, even better, if you identify a constraint around another control, can you do work to elevate that constraint for the business?

WORK SHOULD ALWAYS SUPPORT BUSINESS

- Top line goals of top executives exist for a reason
  - Does your work align to those goals?
  - Does it help those executives meet those goals?
  - If not, WHY ARE YOU DOING IT?
- Understand where controls exist in the business
  - As the keeper of the IT controls, are you responsible for catching everything?
  - What other controls exist in the business that you can leverage to avoid putting work into the system?
  - Or, even better, if you identify a constraint around another control, can you do work to elevate that constraint for the business?

HOW DO YOU SUPPORT THE BUSINESS?

- Infuriating platitude: “Infosec needs to enable the business”
  - Goal: Grow European business by 20% Y/Y
  - Response: Because we are good at information security, we can run the business at a lower fraud rate and take on riskier (and more lucrative) business than our competitors
- Going from “mythical, consultant-sounding speak” to actions is hard.

SELLING INFOSEC

- Pride before fall, fall before redemption
- Offense is profit center (NFL: scoring points on board; projects)
  - Steal market share, acquiring companies
  - Investing in new products (giving budget)
  - Diversify or enable new channels/markets
- Defense is a cost center
  - Exclusive use of scarce resource or supply chain resource
  - Divesting business to protect the core (getting rid of POS system); Business waste

BUSINESS ALIGNMENT EXAMPLE

Performance Measures	Area of IT Reliance	Business Risk Due to IT	IT Controls Relied Upon
1. Understanding customer needs and wants			
2. Product portfolio			
3. Time to market (R&D)			
4. Sales forecast accuracy			
5. Sales pipeline			
6. Customer on-time delivery			
7. Customer retention			

BUSINESS ALIGNMENT EXAMPLE (CONT.)

Performance Measures	Area of IT Reliance	Business Risk Due to IT	IT Controls Relied Upon
1. Understanding customer needs and wants	Order entry and inventory management systems		
2. Product portfolio	Order entry systems		
3. Time to market (R&D)	Phoenix		
4. Sales forecast accuracy	(same as #1)		
5. Sales pipeline	CRM, marketing campaign, phone/voicemail, MRP systems		
6. Customer on-time delivery	CRM, phone/voicemail, MRP systems		
7. Customer retention	CRM, customer support systems		

BUSINESS ALIGNMENT EXAMPLE (CONT.)

Performance Measures	Area of IT Reliance	Business Risk Due to IT	IT Controls Relied Upon
1. Understanding customer needs and wants	Order entry and inventory management systems	Data not accurate, reports not timely and require rework	
2. Product portfolio	Order entry systems	Data are inaccurate	
3. Time to market (R&D)	Phoenix	three-year cycle time & WIP makes clearing IRR hurdle rate unlikely	
4. Sales forecast accuracy	(same as #1)	(same as #1)	
5. Sales pipeline	CRM, marketing campaign, phone/voicemail, MRP systems	Sales mgmt can't view/manage pipeline, customers can't add/change orders	
6. Customer on-time delivery	CRM, phone/voicemail, MRP systems	Customers can't add/change orders	
7. Customer retention	CRM, customer support systems	Sales cannot manage customer health	

BUSINESS ALIGNMENT EXAMPLE (CONT.)

Performance Measures	Area of IT Reliance	Business Risk Due to IT	Controls Relied Upon
1. Understanding customer needs and wants	Order entry and inventory management systems	Data not accurate, reports not timely and require rework	Need input validation to prevent bad data from Marketing Need weekly reporting capability
2. Product portfolio	Order entry systems	Data are inaccurate	Need testing of automated controls to ensure integrity of data
3. Time to market (R&D)	Phoenix	three-year cycle time & WIP makes clearing IRR hurdle rate unlikely	Need better review of new projects to ensure business goals achievement likely
4. Sales forecast accuracy	(same as #1)	(same as #1)	
5. Sales pipeline	CRM, marketing campaign, phone/voicemail, MRP systems	Sales mgmt can't view/manage pipeline, customers can't add/change orders	Need better change and configuration controls around app and environment
6. Customer on-time delivery	CRM, phone/voicemail, MRP systems	Customers can't add/change orders	Loosen report controls to allow managers to add/modify reports
7. Customer retention	CRM, customer support systems	Sales cannot manage customer health	Change control & sec reviews to ensure uptime

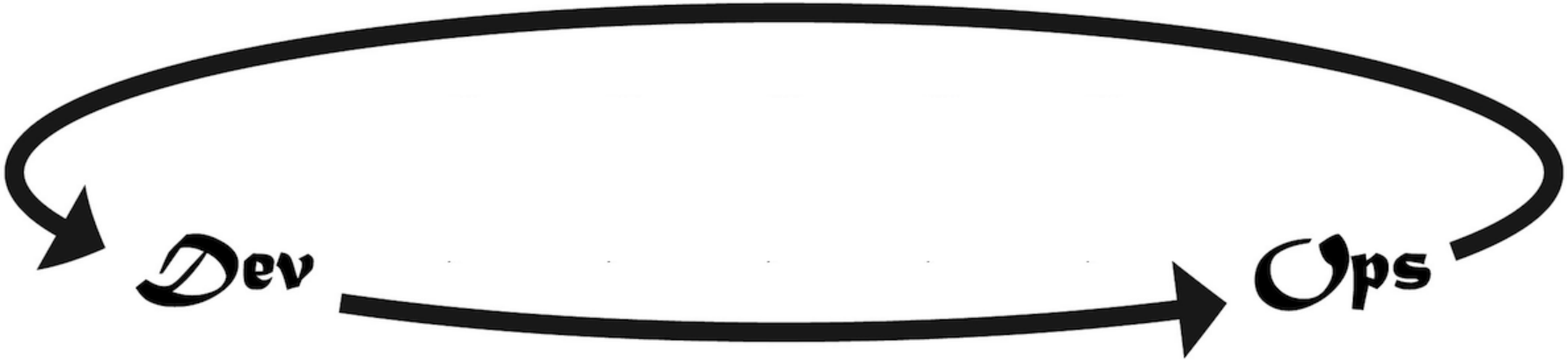
Exercise: Compare

- Resulting infosec program

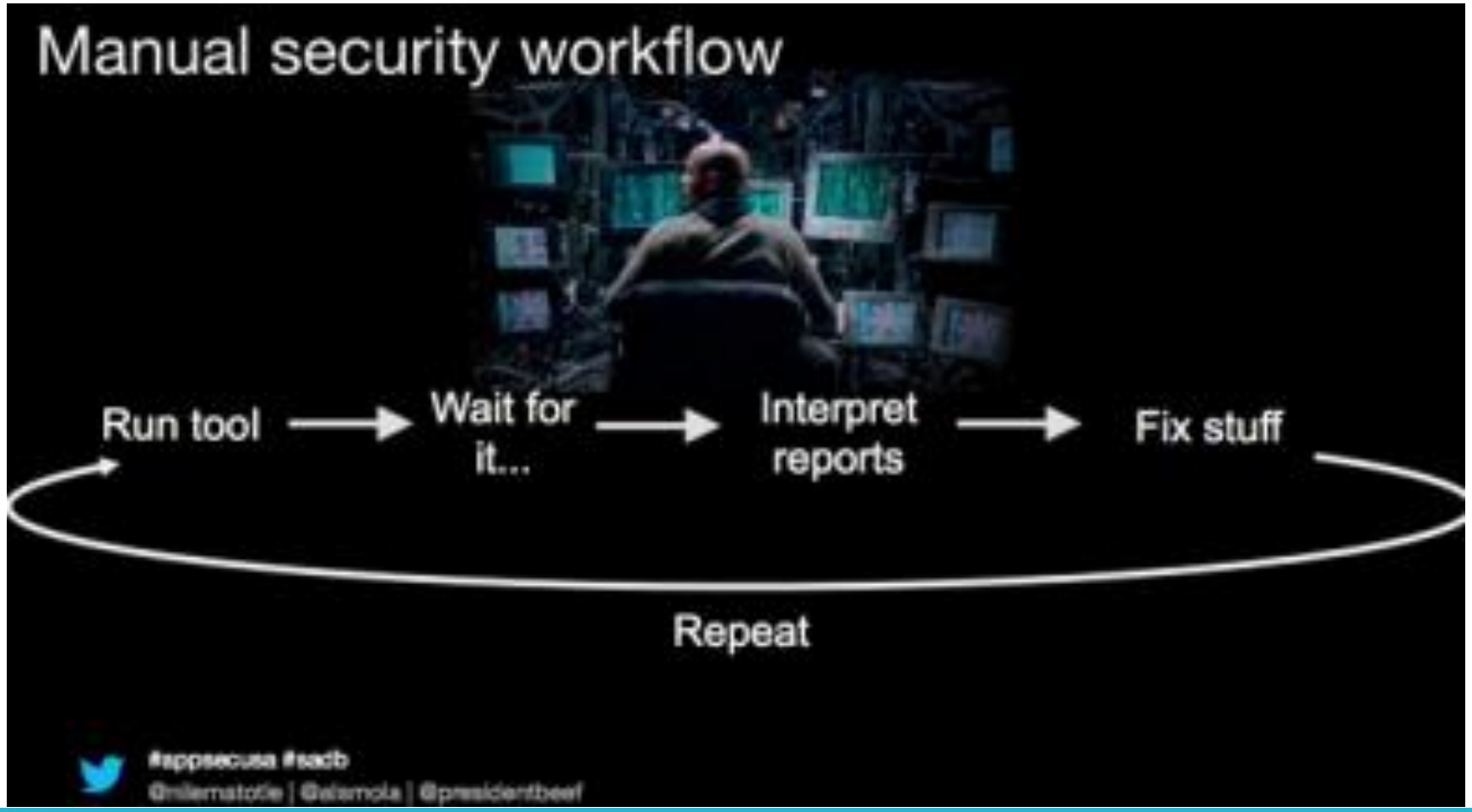
- Vs. Typical Infosec program
  - Respond to audits
  - Prepare for audits
  - Convince IT Operations to implement patches

THE SECOND WAY: AMPLIFY FEEDBACK LOOPS (R TO L)

- Understand and respond to the needs of all customers, internal and external
- Shorten and amplify all feedback loops: stop the line when necessary
- Create quality at the source
- Create and embed knowledge where we need it



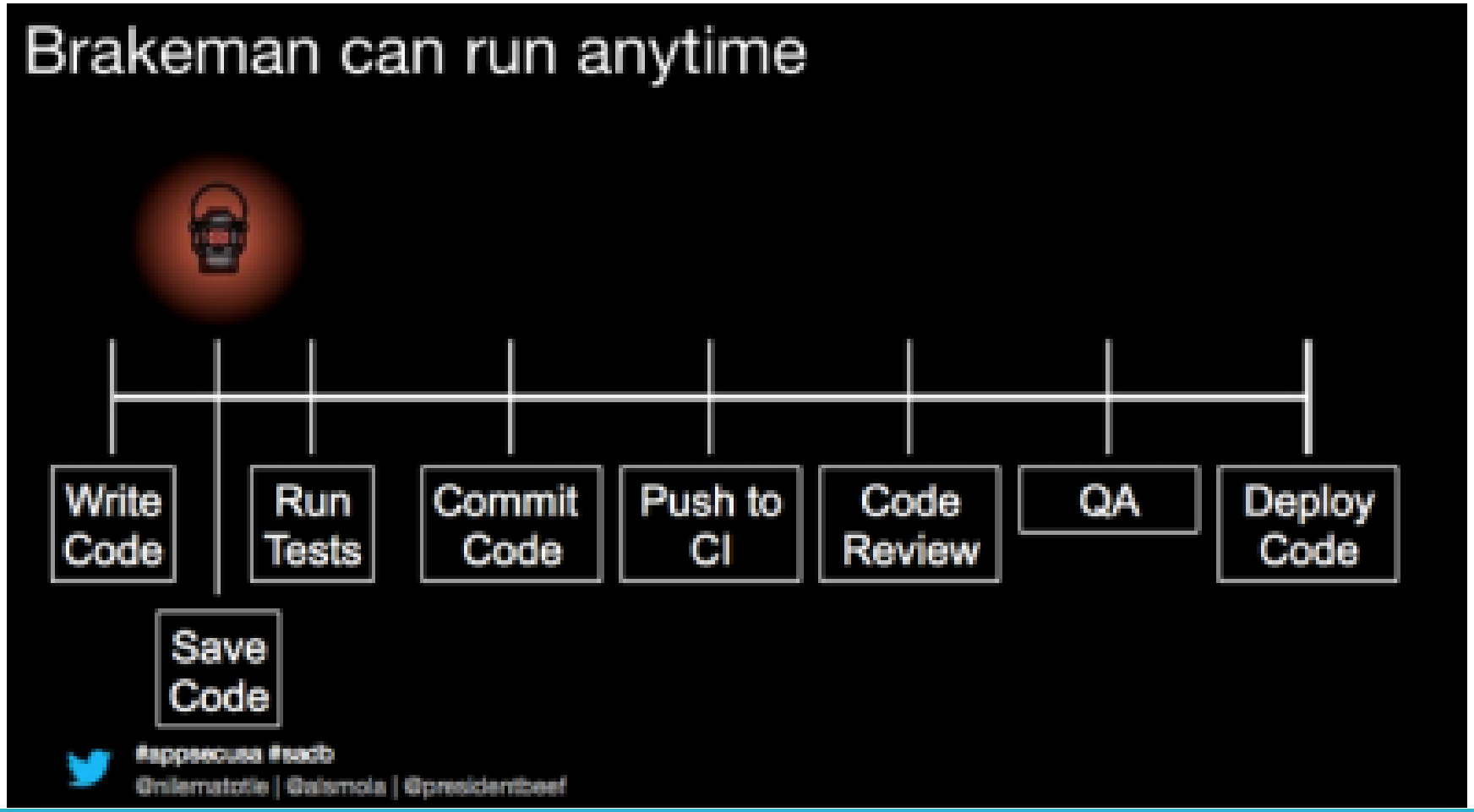
THE TWITTER INFOSEC PROGRAM



WHAT THE TWITTER INFOSEC TEAM DID

- They integrated brakeman into the Dev continuous integration process
- It does static code analysis upon ‘code commit’ or even ‘developer save’
- It emails them whenever a vulnerability is found, along with instructions on how to fix it
- It send them a congratulation email when the developer fixes the vulnerability

STATIC CODE ANALYSIS EARLY

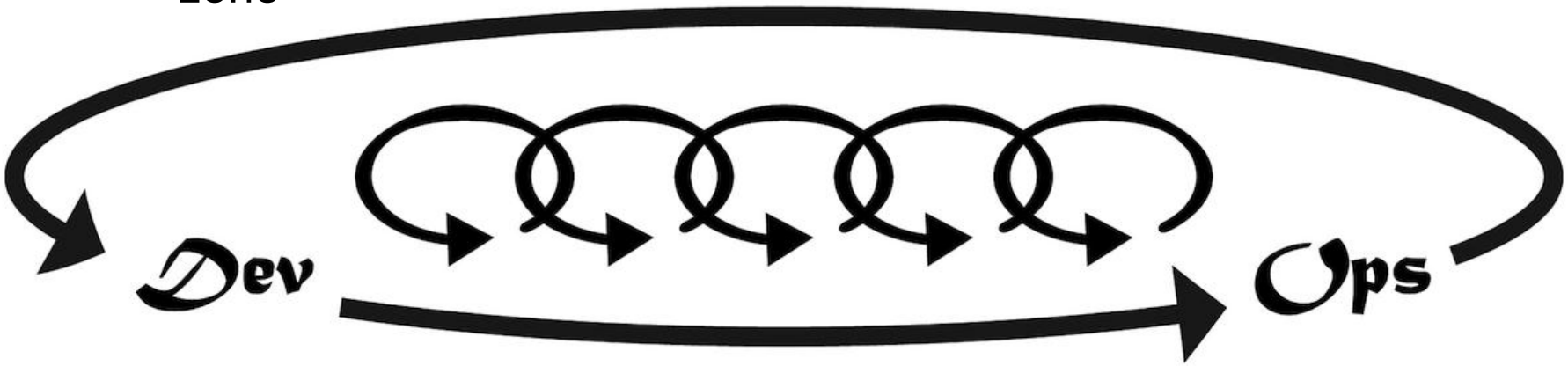


OUTCOMES

- Developers get immediate feedback: issues are found and fixed earlier
- We've encoded our expertise into the automated testing framework
- We've reduced our workload

THE THIRD WAY: CONTINUAL EXPERIMENTATION

- Foster a culture that rewards:
  - Experimentation (taking risks) and learning from failure
  - Repetition is the prerequisite to mastery
- Why?
  - You need a culture that keeps pushing into the danger zone
  - And have the habits that enable you to survive in the danger zone



WHOOPS!

Amazon EC2 outage downs Reddit, Quora

@SCVNGR
SCVNGR

The sky is falling! Amazon's cloud seems to be down (raining?) so we're experiencing some issues too. Be back soon!

5 hours ago via web

Retweeted by RealAmandaStone and others

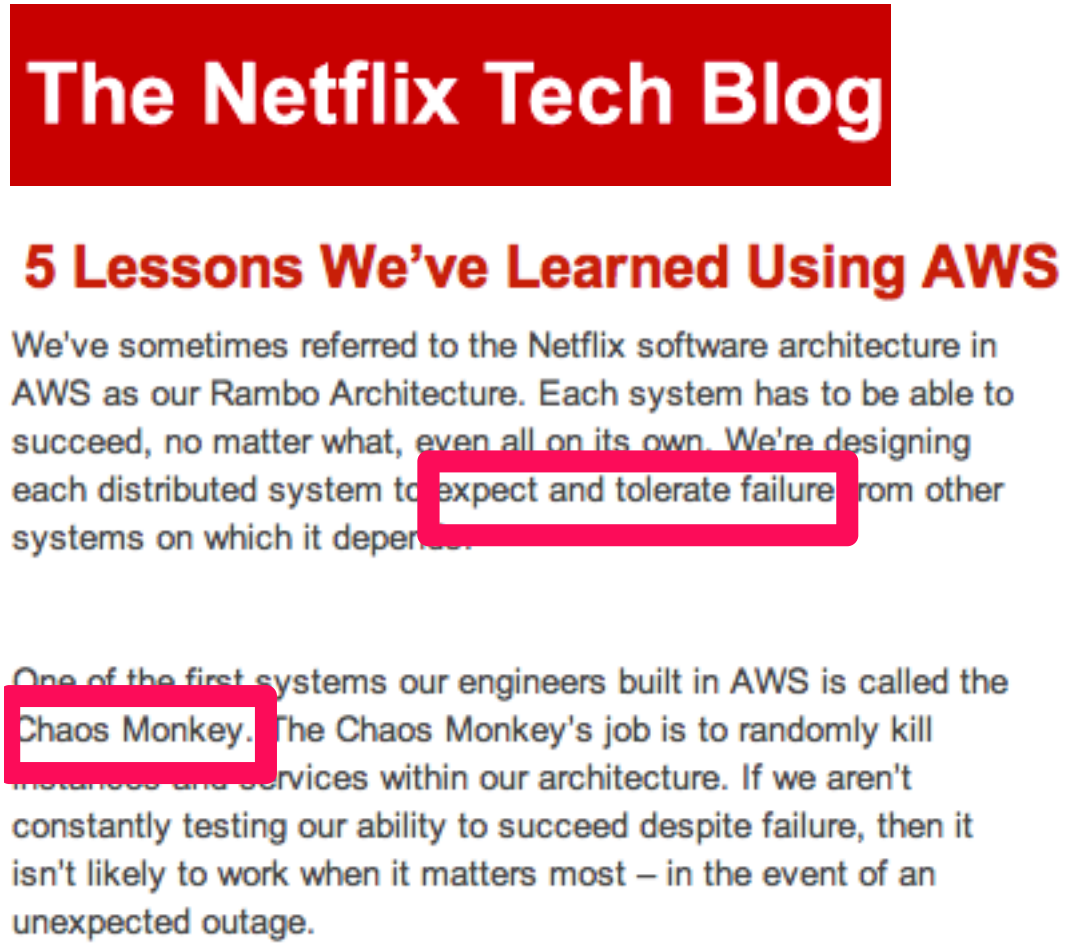
SCVNGR and other sites took to Twitter after a rare and major outage of Amazon's cloud-based Web service.

Recommend 965 people recommend this. Be the first of your friends.

By Julianne Pepitone, staff reporter April 22, 2011: 7:29 AM ET

NEW YORK (CNNMoney) -- A rare and major outage of Amazon's cloud-based Web service on Thursday took down a plethora of other online sites, including Reddit, HootSuite, Foursquare and Quora.

INJECT FAILURES OFTEN



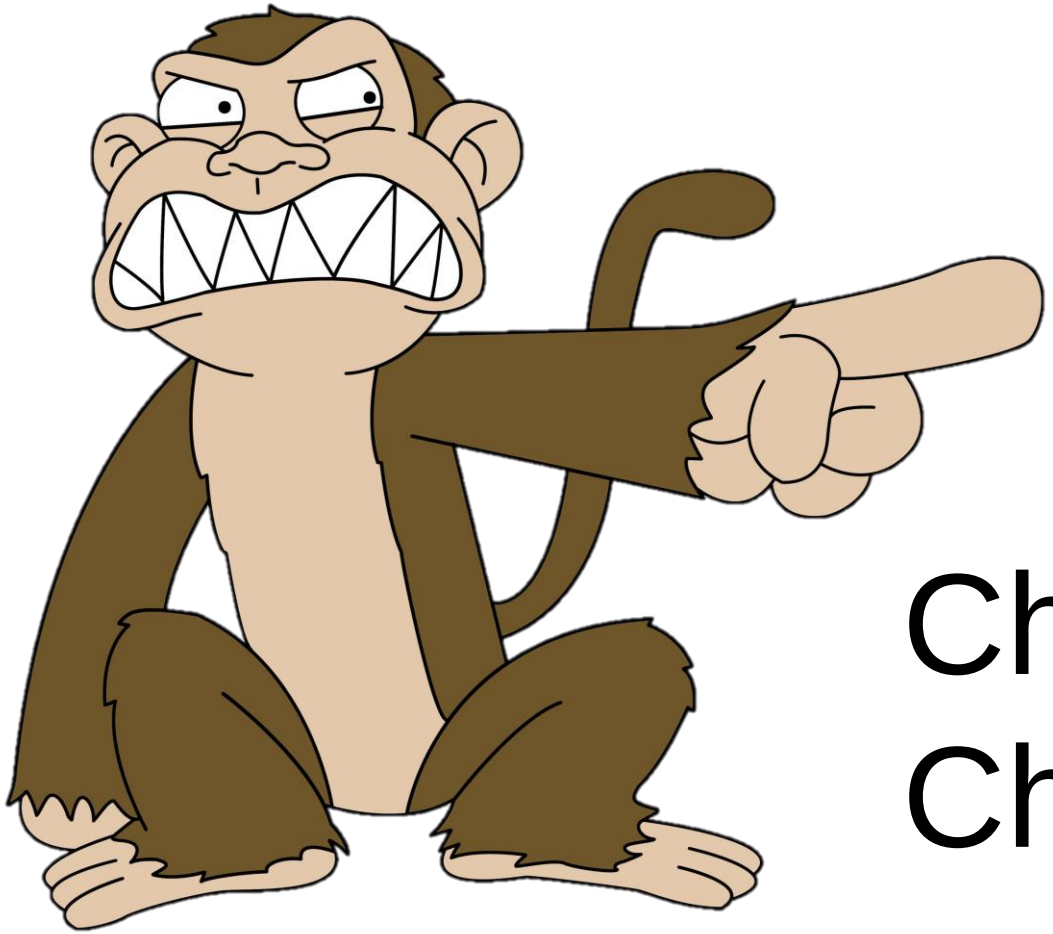
The Netflix Tech Blog

5 Lessons We've Learned Using AWS

We've sometimes referred to the Netflix software architecture in AWS as our Rambo Architecture. Each system has to be able to succeed, no matter what, even all on its own. We're designing each distributed system to expect and tolerate failure from other systems on which it depends.

One of the first systems our engineers built in AWS is called the Chaos Monkey. The Chaos Monkey's job is to randomly kill instances and services within our architecture. If we aren't constantly testing our ability to succeed despite failure, then it isn't likely to work when it matters most – in the event of an unexpected outage.

YOU DON'T CHOOSE CHAOS MONKEY…

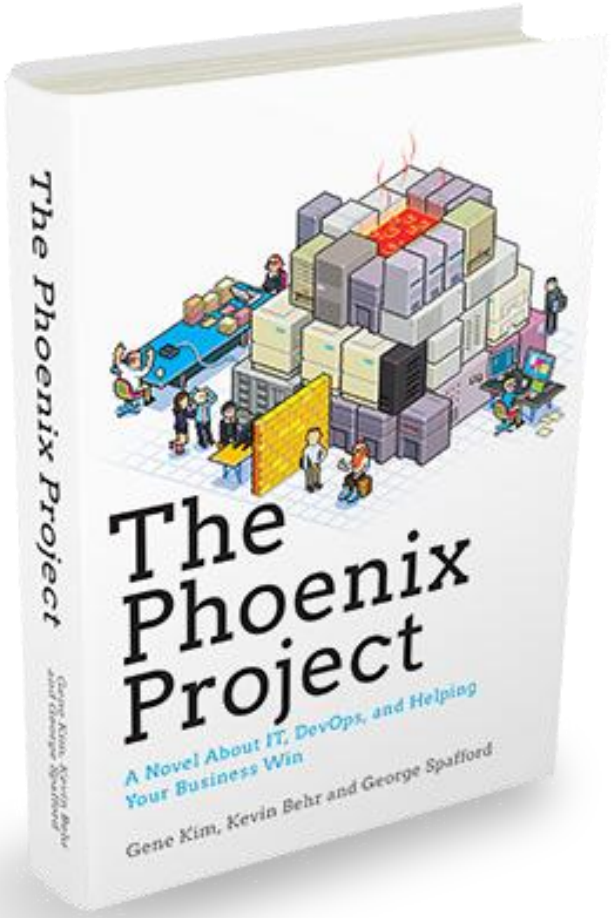


Chaos Monkey
Chooses You!

OUTCOMES

- Defects and vulnerabilities are fixed faster than ever
- Surface area of risk keeps shrinking
- Infosec activities integrated into the daily work of Dev and IT Operations
- Technical debt is finally paid down
- Information security risk has been reduced
- Infosec recognized as helping the business win
- More budget and staff given to infosec

THE PHOENIX PROJECT



QUESTIONS?

Gene Kim
@realgenekim

Branden R. Williams
@brandenwilliams
http://hirebranden.com

Starting With The Business Goals

The KRI Catalog

Business Aspect	Outcomes	Key Risk Indicators				
Demand Management	Market Responsiveness	Channel Costs	Marketing	On-line reputation	Transparency	
	Sales Effectiveness	Lost Sales	Forecast Inaccuracy	Lost Customers		
	Product Development Effectiveness	Product Management	R&D Failure	Aging Products		
Supply Management	Customer Responsiveness	Service Performance	Privacy	Returns	Material Quality	Late Delivery
		Agreement Effectiveness	Customer Care Failure	Order Fill Failures	Service Inaccuracy	
	Supplier Effectiveness	Enterprise Sourcing	Supply Chain Planning	Vendor Risk Management	Supplier Agreement Effectiveness	Supplier Service Performance
	Operational Efficiency	Risk Management	Strategic Planning	Internal Controls	Quality Management	
		Asset Management	Business Continuity Management	Facilities Management	Manufacturing	
Support Services	Human Resources Responsiveness	IT Workforce	Skills Inventory	Identity and Access Management	Training	
	Information Technology Responsiveness	Applications	Infrastructure and Operations	Information Security	IT Investment	Service Level Effectiveness
		Change Management	Cloud	Project and Portfolio Management	Availability	Internal Audit (IT)
	Finance and Regulatory Responsiveness	Compliance	E-Discovery	Environmental, Health and Safety	Internal Audit (Finance)	Records Management
		Governance	Insurance	Ethics	Financial Integrity	
		Legal	Liquidity	Policies	Sustainability	

Gartner

GARTNER RISK-ADJUSTED VALUE MGMT

- Contact Paul Proctor, Chief of Research, Risk and Security, Gartner, Inc. (mailto:paul.proctor@gartner.com)
- Or your Gartner rep

THANK YOU!