



# Lessons Learned from a Bank Moving 100% to the Cloud

Steve Lodin

Sr. Director, Cyber Security Operations  
Sallie Mae

March 26, 2020

---

## Audience Poll

Select your cloud experience

Newbie – just learning about the cloud

Dipping our toes in the water – limited cloud

Fully in – majority of our applications and data center assets are in the cloud

# Agenda

## Moving our Datacenter 100% in the Cloud

- Background
  - ☐ Company
  - ☐ IT
- Golden Rules
- Cloud Migration Observations
  - ☐ Gotchas
  - ☐ Surprises
  - ☐ Lessons Learned
  - ☐ Strategic Changes
- What's next?

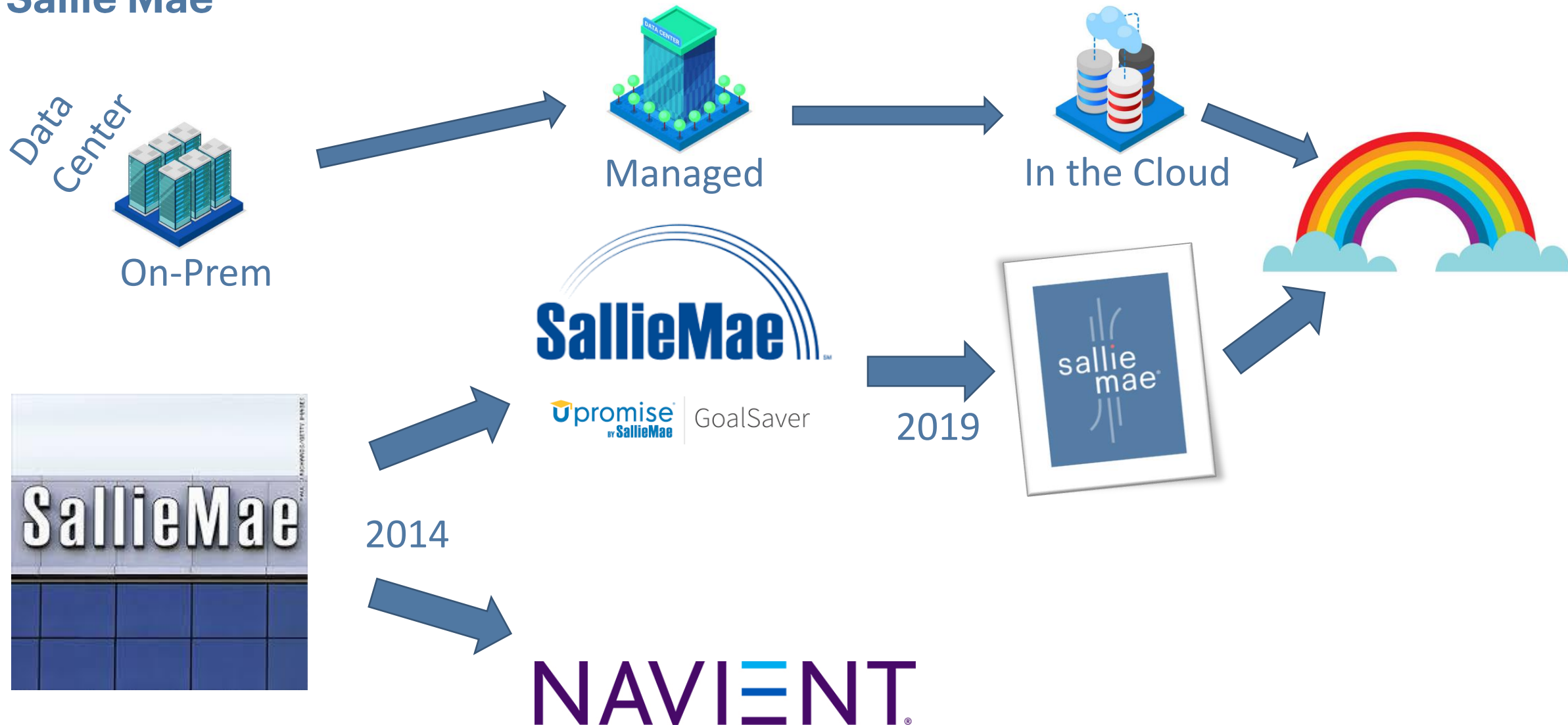
We are a fast follower



---

- **Sallie Mae Background**

# Sallie Mae



## We are a Bank!

60	Valley National Bank	\$	32,999,351
61	Frost Bank	\$	31,882,004
62	Iberiabank	\$	31,359,489
63	CIBC Bank USA	\$	30,860,849
64	Sterling National Bank	\$	30,183,934
65	Texas Capital Bank	\$	29,940,219
66	Sallie Mae Bank	\$	29,485,766
67	Webster Bank	\$	28,957,456
68	Hancock Whitney Bank	\$	28,747,696
69	Umpqua Bank	\$	27,950,817
70	BNY Mellon	\$	27,660,000

<https://www.mx.com/moneysummit/biggest-banks-by-asset-size-united-states>

Corporate Security Team

“Let me remind you: We are a bank”

## TOP 100

Best Savings Accounts & Rates - June 2019				
Account:		Minimum for APY:	APY:	
 BBVA ★★★★☆ \$10,000 minimum balance to receive rate Money Market Account		\$10,000	2.40% Jun 14, 2019	<a href="#">Open Account</a>
 Citi ★★★★☆ 2.36% APY & no min. deposit. Offer available in select markets. Savings Account		\$0	2.36% Jun 14, 2019	<a href="#">Open Account</a>
 Sallie Mae ★★★★★ Money Market Account		\$0	2.30% Jun 14, 2019	<a href="#">Open Account</a>
<a href="#">+ Show More</a> <span>All Listings are Member FDIC</span>				

Savings Rates Provided By Bankrate.com | Advertiser Disclosure

## Bank Systems Overview

*SLM Bank leverages a mix of 3<sup>rd</sup> party / hosted services and internally developed applications*

### Core Systems

- Internal/External existing platforms
- *Upromise – Rewards Program now on Salesforce.com*
- *Credit card processing platform using a FinTech*

### Data Centers

- Primarily consuming IaaS from AWS
- We leverage one region as our primary site and replicate data and server templates to another region for DR capabilities

Migration Strategy  
Lift & Shift

### Infrastructure

- Datacenter – Primarily AWS from the one region
- Telephony - (Call Center/IVR/Dialer) Hosted by 3rd Party
- Office 365 – e-mail / collaboration

---

- **Golden Rules**



# Sallie Mae Cloud Challenges

Struggles we faced as we were migrating from On-Prem to Cloud; regulator buy-in, internal risk acceptance, security visibility, maintaining the defense-in-depth security stack

It's better to prove we are safe and protected following compliance guidelines, traditional audit controls that requires us to have a SIEM, Web Proxy, WAF and IPS, couldn't do that with all native given adoption timeline.



## Golden Rules

### Make IT systems and applications harder to penetrate

- Protect administrative access with Software Defined Perimeter
- Microsegmentation to protect applications and prevent lateral movement
- Perform Basic Hygiene (in other words, stop stupid)
  - No public S3 buckets
  - No over-permissioned security groups
  - Every new S3 bucket has logging enabled and is encrypted
- CIS Security Benchmarks used as compliance stick
- MFA for cloud infrastructure administrative accounts



## Golden Rules

### Make IT systems, applications, and data harder to co-opt or pwn

- Encrypt everything at rest
- Encrypt sensitive data and transactions in motion
- DLP where possible
- Common security framework for all generated servers
- Protect administration accounts and privileges

*the*  
**GOLDEN RULE**

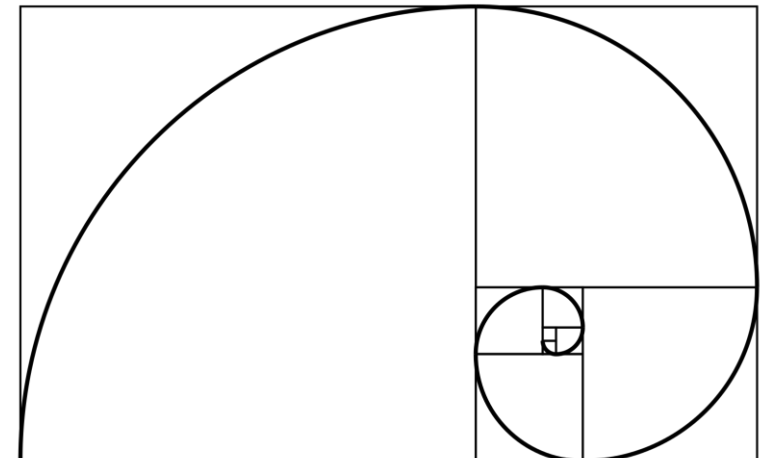
# Golden Rules

## Make attacks harder to conceal

- Centralize logging where possible to ensure logs are collected, shared to analysis tools, and archived
- Monitor Cloud Operations (i.e., Dome9/RedLock/Evident.IO/AvidSecure)

## Make effects of attacks and compromise easier to recover from

- Ensure forensics tools can run on all IaaS systems
- Ensure system and data backups are recoverable
- Create immutable systems
- Blue/Green system implementation



# Golden Rules

## Make Effective Operational Foundations Prior to Migration

- Automate where possible, infrastructure-as-code
- Eliminate console servers → Cloudify either by Native Solutions or SaaS applications
- No (or minimal) changes during the Lift & Shift unless the workload is eliminated, replaced, or cloudified
- No special snowflakes



**GOLDEN  
RULE**

---

- **Migration Observations**

## Gotchas

- IT Operational Logging is necessary, it's hard to figure out what's necessary and what's broken during the migration without it
- AWS Security Groups are not a next generation application security firewall
- AWS Load Balancers do not have the same features as on-prem load balancers
- Compliance testing and evidence gathering during the migration was challenging



## Surprises

- AWS Security Groups have limits
- Characterizing Network Utilization for Microsegmentation was harder than expected
- Native Network IDS/IPS and SPAN Ports and Tapping was not available in AWS,\* we needed a story for regulatory controls like PCI
- Many core security vendors are not experienced for environments fully in the Cloud
- Security visibility can increase with forced/available cloud logging, but it has an impact on EPS-driven vendor products



\* Tapping is available as we speak with AWS Mirror



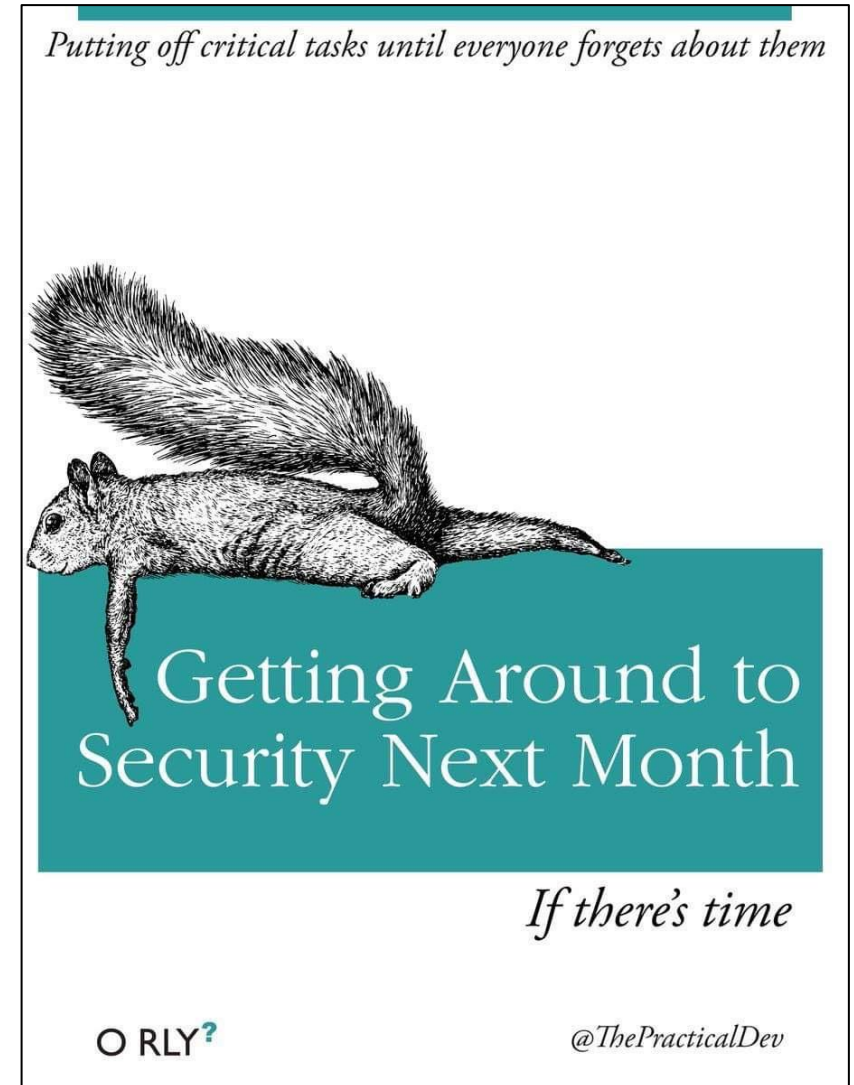
## Lessons Learned

- Combining multiple major IT changes at the same time - bad
- Start small, automate where possible, properly size assets
- No cloud infrastructure accounts outside managed accounts under billing
- Governance over Amazon AWS services
  - Request/approval process
  - Cost management
  - Least privileges/separation of duty
  - Automation
  - Controls development
- Accurate Tagging is critical



## Lessons Learned

- Challenges with AWS training for developers
- Sandbox development environments are challenging
- Encountered skills issues in the area
- Involve Compliance early and plan for extra time
- Don't abandon the Change Management process
- Don't trust the backlog



# Strategic Changes

## Pre-Migration

- Early involvement with regulators, understand what their requirements for the cloud are
- Early change from Azure to AWS

## During Migration

- New Infrastructure Management with operational and security changes

## Post Migration

- Logging Strategy
- Dev/Sandbox Strategy



# Strategic Changes


## Next Generation

- Immutability and consumable assets
- Chargeback
- Disaster Recovery → Resilience
- Crawl -> Walk -> Run → IaaS -> Containers -> Serverless -> Multi-cloud
- Account Strategy → 20 -> 200
  - Based on new Amazon strategy and presentations at Re:Inforce
  - Enables cleaner future chargeback and microsegmentation



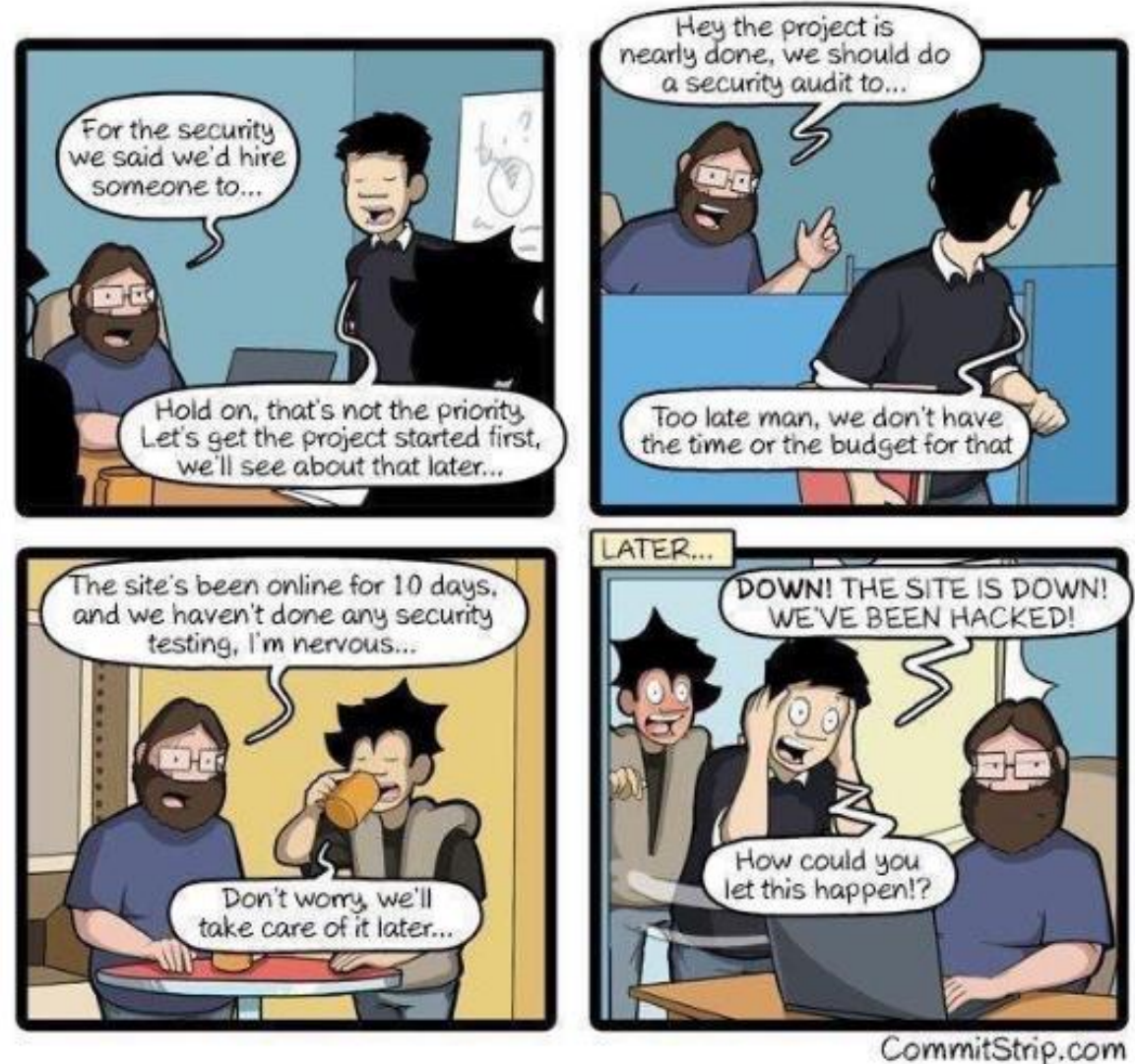
## What's next?

### Application Modernization Strategy

Rehost	"Lift and Shift" to like infrastructure in the cloud 
Rebuild	Match existing business function with a new solution in the target modern, cloud native architecture
Rearchitect	Make architectural changes moving the application to the desired target modern, cloud native state
Revise	Enhance the application over time by increasing the level of craftsmanship, DevOps and cloud scalability
Replace	A commodity or turnkey SaaS solution is available to meet the business need
Retire	The application is no longer required or has already been replaced

## Let's hope you don't hear this

- It's Too Hard.
- We'll get to that later.
- Can I have an exception?
- Ohhh, is that S3 bucket Public?





Questions?

Thank you!

 Steve.Lodin@salliemae.com

 @stevelodin

 <http://www.linkedin.com/in/stevelodin>