ACUIA
Association of Credit Union Internal Auditors

28th Annual Conference and One Day Seminar

Internal Audit Are You in the Cloud?

Catherine Bruder, CPA, CITP, CISA, CISM, CTGA, SOC
IT Consultant
June 22, 2018

DoerenMayhew
CPAs AND ADVISORS

Objectives

- ✓ Identify key drivers for credit unions moving to the cloud
- ✓ Recognize the role internal audit plays in the cloud strategy
- ✓ Analyze the complexities and unique risks associated with a cloud strategy
- ✓ Differentiate changes in the internal audit plan to act as an advocate for a strong cloud strategy
- ✓ Apply the same rigor to the cloud to remain within the institutions risk tolerance

The Amazon Effect

Institutions are relying on new technologies to cater to changing consumer attitudes.

Harland Clarke Report, May 2018

Consumers want more faster

Even when it comes to non-app interactions, consumers want more, faster:

- 81% demand an increased response time[1]
- A two-second delay in webpage load time leads to a 20% abandonment rate[2]
- 59% of consumers want personalized offers and service[3]

1. IBM Institute for Business Value Report, 2016
2. "7 Scary Stats for Ecommerce Retailers," Shopify, December 21, 2016
3. Ibid

How are CUs Catering to Members?

Instant card issuance is a large part of the answer because it attracts customers, supports in-branch banking, and enhances customer loyalty.

- 36% of millennials and 47% of 18 to 24-year-olds say instant issuance impacts their decision on where to bank[4]
- By 2020, over half of financial institutions will have an instant issuance solution

4 Alte Group

Gartner Says By 2020

- "A Corporate "No-Cloud" Policy Will Be as Rare as a "No-Internet" Policy Is Today"
- Hybrid cloud adoption grew 3X in the last year, increasing from 19% to 57% of organizations surveyed
  - Private
  - Public
  - Hybrid

5 Reasons Cloud Technology = Great Idea

Enhanced Data Security

- Data security is a high priority
- Data is stored remotely, securely and redundantly
- Not only stores critical system and member data in the cloud but also documents and images

IT Staff Efficiency

- Will generate operational efficiencies and provide cost-savings in the long run
- Free up your IT staff to work on member-facing improvements or projects
- Eliminate daily maintenance and reduce disaster recovery planning

5 Reasons Cloud Technology = Great Idea

Reduce Cost of Replacing Outdated Software and Hardware

- Receive new hardware and operating system upgrades regularly
- Keep up with the latest operating system

Training by Experts Who Know the Product

- IT support and education on new releases or updates
- Training for your staff by experts
- On-call and available resources to help troubleshoot

Cost-effective and Reliable

- Data centers that have highly redundant connectivity, reliable backup generators, no single point of failure
- The staff expertise in the case of a disaster or disruption in uptime.
- Access to your data, automatic back up, and seamlessly accessible from your desktop

5 Credit Unions Considerations

Considerations Before You Leap to the Cloud

Overleveraged

- Smaller cloud providers may be running at the limits of their current system, not wanting to spend more on costly upgrades

Underperformance/Latency

- It's not just static data the gets moved to the cloud. Dynamic data that has to move back and forth with as little latency as possible

NAFCU Services, Gregg Early, Strategic Content Director, Geezeo, March 12, 2018

5 Credit Unions Considerations

Considerations Before You Leap to the Cloud, continued

Data without Action

- Tools to slice and dice the data you receive from your members and turn it into actionable strategies

Mobile Reliability

- Reliable cloud services firm is crucial.

Configurations

- Changing cloud providers requires time because each cloud service and its partners have different protocols so pick a partner to stick with

NAFCU Services, Gregg Early, Strategic Content Director, Geezeo, March 12, 2018

5 Key Requirements for Cloud

1) Ease of Use
2) Open Source Friendliness
3) Cost
4) Technical Support
5) Strong Partner Ecosystem

3 Cloud Migration Mistakes

No. 1: Doing pure “lift and shift”

- Moving applications and data making little or no modifications.
  - Cloud-based applications need to have some cloud-native localization.
  - Need to use the public cloud platform in optimal ways, to reduce operational cost and increase performance.
  - Not making the modifications for the change, the application is 30 to 40 percent less efficient. [5]

3 Cloud Migration Mistakes

Mistake No. 2: Not dealing with data

- Not dealing with the issues around the database until after migration.
- The tendency is to pick pretty much the same database, you end up spending way too much on the database in the cloud.
- Look at migrating to a better database in the cloud.
- Consider databases created in the cloud, if you can. [5]

3 Cloud Migration Mistakes

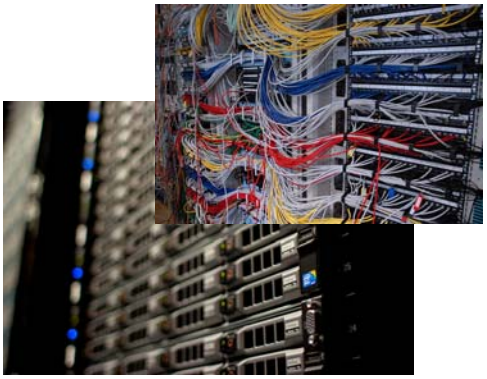
Mistake No. 3: Avoiding or delaying integration with development / operations

- There can be a disconnect as to how cloud meets the devops tool chain and processes.
- This huge mistake can cost millions in lost productivity.
- Do application development and operation in the cloud, and you can couple devops tools chains, testing, and deployment with cloud-based services.[5]

5 "Cloud Computing", InfoWorld, David Linthicum, Jun 15, 2018

The Cloud

- Security as a Service
  - IDS/IPS, monitoring, etc.
- Application Service Providers
- Cloud Infrastructure
- Virtual Placement of Servers
- Computing Environment
- Supplementing CUs own Servers



The Role of Internal Audit

WHAT SHOULD YOU BE DOING

New Ways to Assess Risk

Risk in Dynamic Nature of the Cloud

- The location of the processing facility may change according to load balancing
- The processing facility may be located across international boundaries
- Operating facilities may be shared with other entities
- Legal issues (liability, ownership, etc.) relating to differing laws in hosting countries may put data at risk

Residual Risk

- The credit union can reduce residual risk by offloading a portion of the responsibility for managing IT risks to a cloud service provider
- IA should recognize this valuable opportunity while addressing the new risks that are introduced
- Advocate a strong cloud strategy that is within the risk tolerance of the credit union

Not Just Another Third-Party Vendor

Cloud environment has its own complexities

- SOC Reports and other attestation reports valuable but should be only the initial step in the IA process
- Not just vendor management
- No two clouds are the same
- Third-party vendor barriers

Third-Party Barriers

- Auditing the cloud provider may not be an option
  - SOC 1, 2 and 3 as alternatives
  - Consider this before contracting with a cloud vendor

Shared Control Responsibility

In reality, controls are required by both the cloud provider and the credit union

- IA must determine which controls reside with the cloud provider and which controls reside with the credit union
- For example
  - ✓ CU is responsible for configuration and access management
  - ✓ Cloud provider is responsible for physical and environmental controls

Risk Assessment Quality

Consider the issues identified in the assessments

Discuss the contents of the risk assessment

Consider

- Reliance on technology
- Presence of member data
- Regulations
- Risk mitigation

Risk Assessment

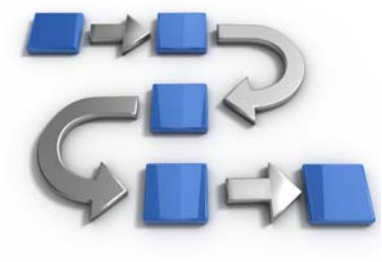
- Strategy
  - ✓ What will the cloud be used for?
  - ✓ What are the expectations for the cloud deployment?
  - ✓ What are the anticipated benefits?
- Personnel
  - ✓ IT training
  - ✓ IA training
- Security Program
  - ✓ What data is stored in the cloud?
  - ✓ What do we need to change?

Risk Assessment

- Vulnerability assessments and penetration testing
  - ✓ Cloud provider contracted or CU contracted
  - ✓ Permission to test must be obtained
    - Complicated because of multiple users in the cloud environment
- Reliability and redundancy
  - ✓ Often a key reason for moving to the cloud environment
  - ✓ How will it be tested?
  - ✓ Is it truly redundant at another location?

Inventory

- Virtualization and optimization by cloud provider
  - ✓ This makes maintaining an inventory to audit much more difficult
  - ✓ Regular system diagrams with data flows help maintain an inventory but will require the cooperation of the cloud provider
  - ✓ Detect shadow IT in the network



Preventative

Cloud providers need to have strong preventative controls

- Configuration management
- Web application hardening
- Internal security (background checks)
- Continuous monitoring
  - Patch management
  - Event monitoring
- Vulnerability scanning

Benchmarking

FINDING A FOUNDATION

IT Security Benchmarking

- Data Classification Policy
  - ✓ Having a method for identifying and classifying data
  - ✓ Defining requirements for accessing and handling data
- FISMA CIO Metrics 2018
  - ✓ Covers governmental agency metrics for cybersecurity
- Cloud Security Alliance
- Choose a Framework
  - ✓ NIST Cybersecurity Framework (FFIEC version)

Cloud Security Alliance

Cloud Security Alliance

Domain 1
- Cloud Computing Concepts and Architecture

Domain 2
- Governance and Enterprise Risk Management

Domain 3
- Legal Issues, Contracts and Electronic Discovery

Domain 4
- Compliance and Audit Management

Cloud Security Alliance

Domain 5
- Information Governance

Domain 6
- Management Plane and Business continuity

Domain 7
- Infrastructure Security

Domain 8
- Virtualization and Containers

Cloud Security Alliance

Domain 9
- Incident Response

Domain 10
- Application Security

Domain 11
- Data Security and Encryption

Domain 12
- Identity, Entitlement, and Access Management

Cloud Security Alliance

Domain 13
- Security as a Service

Domain 14
- Related Technologies
  - Big Data
  - Internet of Things
  - Mobile

Cybersecurity

IT'S RELATIONSHIP TO THE CLOUD

Cyber-Risk

Cyber-risk is REAL

- Viruses, malware, spyware, ransomware
- Not a matter of if but when
- IA is being called upon to help
  - Identify where, when and how the breach occurred
  - Evaluate the effectiveness of the incident response team

Cybersecurity Threats

Data Breaches

143 Million identities

5 Million debit and credit cards

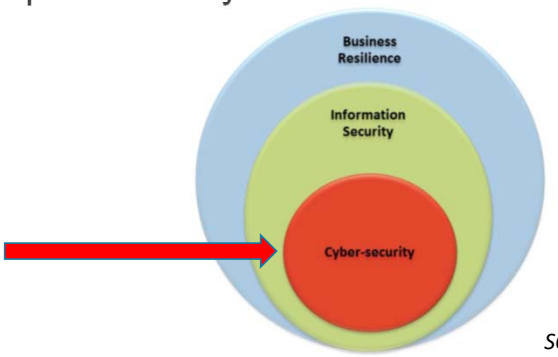
Cybersecurity Threats

Overall, a full 67% of global organizations now report they have suffered a breach at some time in the past, compared with 56% last year.

2018 THALES DATA THREAT REPORT

Cybersecurity

The ability to protect or defend the use of cyberspace from cyber attacks.



SOURCE: CNSSI-4009 - NIST.IR.7298r2

FFIEC Cybersecurity Assessment Tool

AKA – A CLOUD ASSESSMENT TOOL

Cybersecurity Assessment

In 2018, cybersecurity will remain a key focus. The NCUA will begin implementing the Automated Cybersecurity Examination Tool (ACET), which provides the agency with a "repeatable, measurable and transparent process for assessing the level of cyber preparedness across federally insured institutions."

This tool aligns with the Cybersecurity Assessment Tool developed by the FFIEC for voluntary use by credit unions.

The NCUA will begin using the ACET in examination of credit unions with $1 billion or more in assets.

Benefits to the Institution

Enhanced oversight and management of the institution's cybersecurity

- Identifying factors contributing to and determining the institution's overall cyber risk.
- Assessing the institution's cybersecurity preparedness.
- Evaluating whether the institution's cybersecurity preparedness is aligned with its risks.
- Determining risk management practices and controls that are needed or need enhancement and actions to be taken to achieve the desired state.
- Informing risk management strategies.

Assessment Components

The Assessment consists of two parts:

- Inherent Risk Profile
- Cybersecurity Maturity.

Benefit

- Upon completion of both parts, management can evaluate whether the institution's inherent risk and preparedness are aligned

Inherent Risk Profile

Cybersecurity inherent risk is the level of risk posed to the institution by the following:

- Technologies and Connection Types
- Delivery Channels
- Online/Mobile Products and Technology Services
- Organizational Characteristics
- External Threats

Inherent risk incorporates the type, volume, and complexity of the institution's operations and threats directed at the institution

Inherent risk does not include mitigating controls

Cybersecurity Maturity

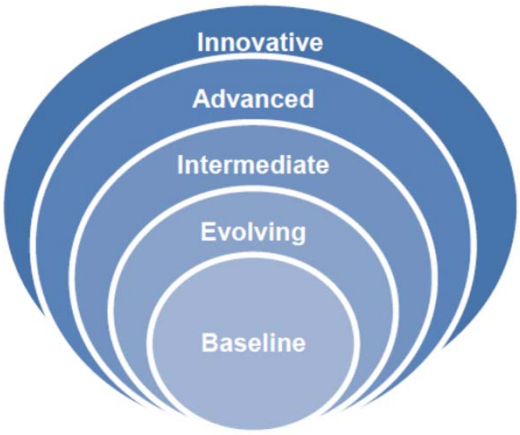
Management then evaluates the institution's Cybersecurity Maturity level for each of five domains:

- Cyber risk management and oversight
- Threat intelligence and collaboration
- Cybersecurity controls
- External dependency management
- Cyber incident management and resilience

Five Key "Domains" for Cybersecurity Preparedness

1. Cyber risk management & oversight
   - Strong governance is essential
2. Threat intelligence & collaboration
   - Strength in numbers
3. Cybersecurity controls
   - More than one kind of control
4. External dependency management
   - Your security starts with their security
5. Incident management & resilience
   - Mitigation and recovery are a must

Maturity Levels



Take-Aways

- Understand your cloud environment
  - ✓ Be a proactive part of the strategy if you can
- Gain an understanding of the risks
- Create an audit plan using a framework and guidance such as NIST and Cloud Security Alliance (CSA)
- Apply the same rigor to your cloud environment to match your credit union's risk tolerance

Thank You!

Catherine Bruder, CPA, CITP, CISA, CISM, CTGA, SOC
IT Consultant
bruder@doeren.com
248-244-3295

DoerenMayhew
CPAs AND ADVISORS