

Questions?

Ben Sady
Director, *Risk Advisory*
Ben.Sady@dhgllp.com

Peter Tsengas
Senior Consultant, *Risk Advisory*
Peter.Tsengas@dhgllp.com



Agenda

- Difference Between Continuous Monitoring & Continuous Auditing
- Drivers for CM & CA
- How CM & CA Can Improve Security Posture
- Examples of CM & CA
- Example Implementation Strategy

CM & CA

Continuous Auditing (CA)

- Audit's responsibility
- Collection of audit evidence by an auditor related to business processes & controls on a continuous basis
- Broader in scope (compared to CM); may include numerous tests & procedures (one component of which may be CM)

Continuous Monitoring (CM)

- Management's responsibility
- CM is a methodology that automatically and regularly queries data to identify errors, irregularities, unusual conditions, fraud indicators, positive trends, and other noteworthy conditions that might not otherwise be detected.



Key
Differences

...basis.
...assessed on a
...the evidence to be
...se monitoring
...ous Auditing to
...systems mu

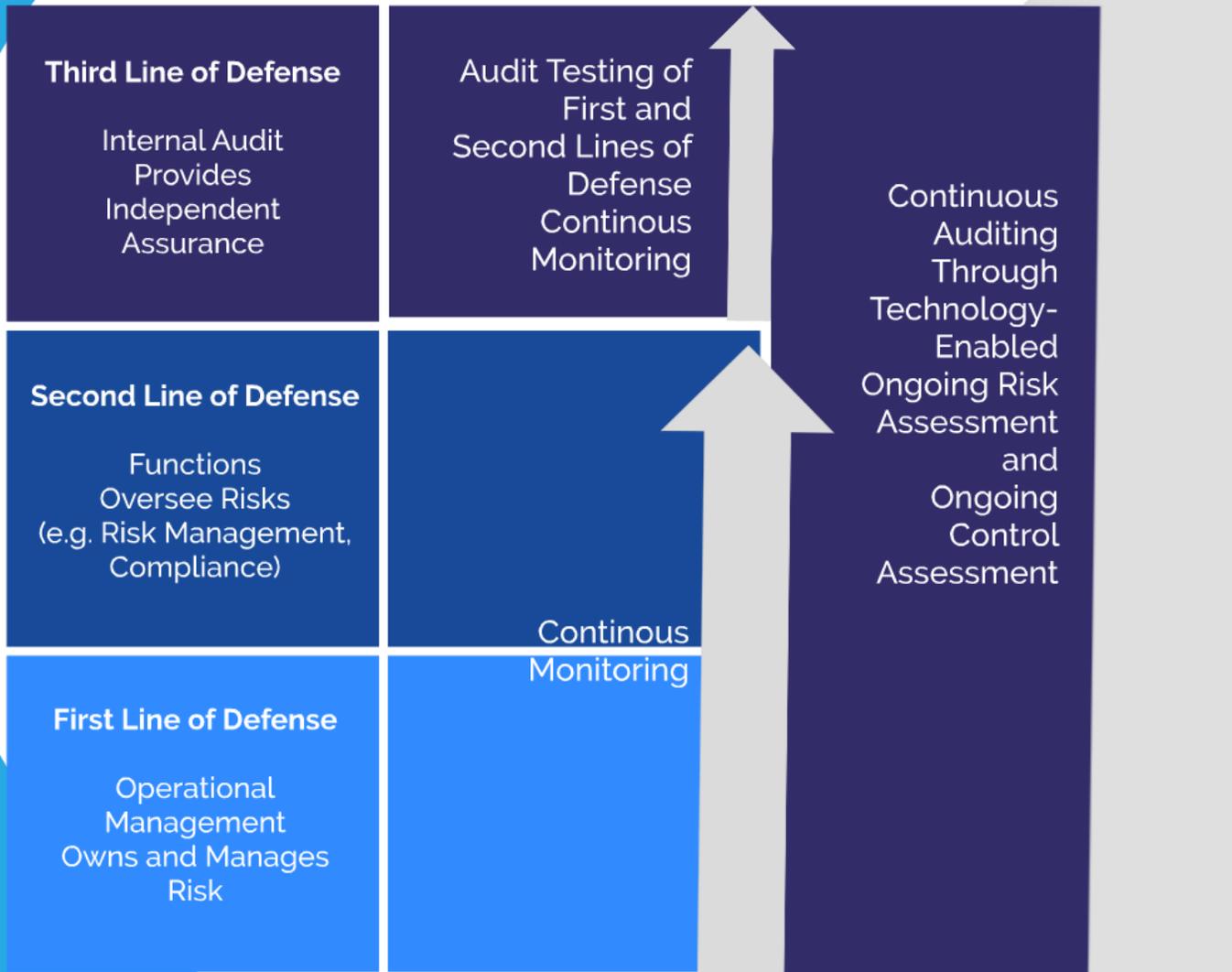
Continuous Auditing can be feasible ***only if*** it is built upon Continuous Monitoring.

Continuous Monitoring systems must be in place for Continuous Auditing to be effective, **as these monitoring systems provide the evidence to be collected and assessed on a continuous basis.**

- otherwise

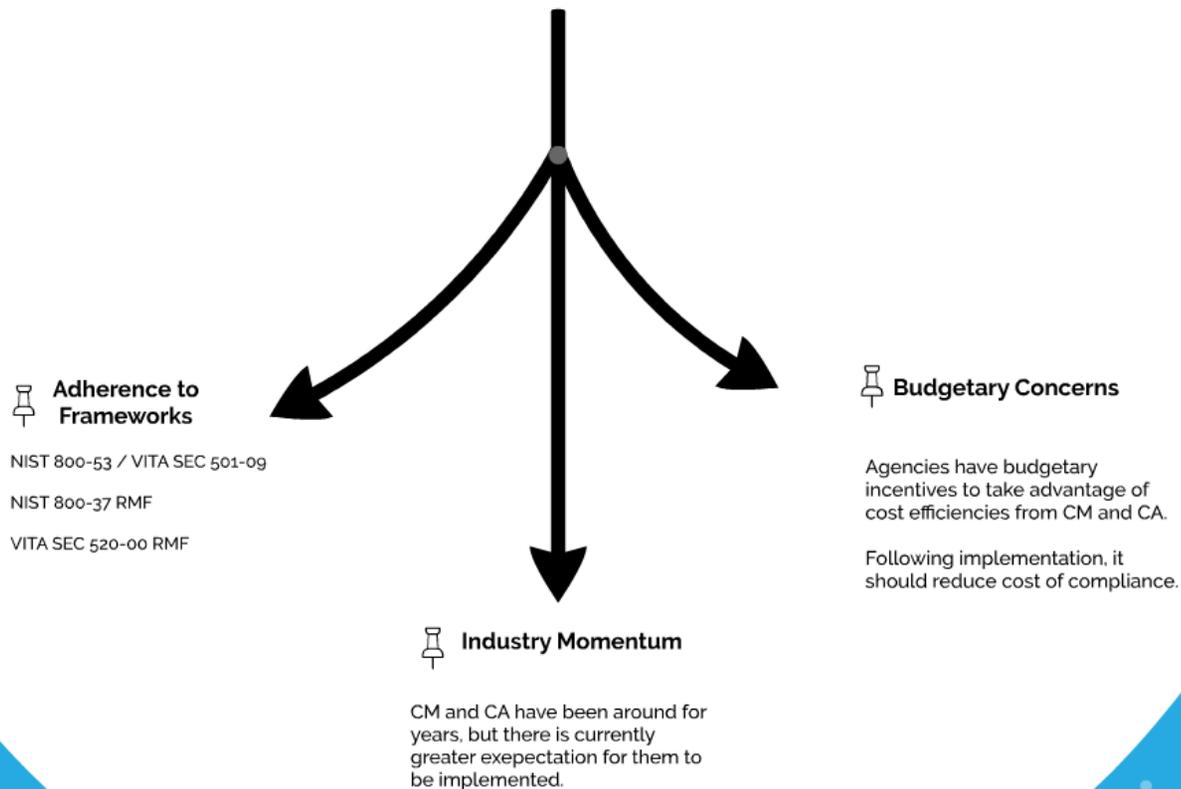
Continuous Assurance achieved through the internal audit activity's:

- Audit Testing of First and Second Lines of Defense Continuous Monitoring
- Continuous Auditing



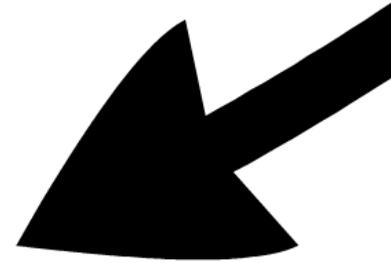
Drivers for CM & CA

Adherence to frameworks and industry momentum are driving the search for **viable CM and CA solutions.**





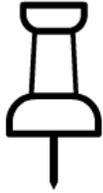
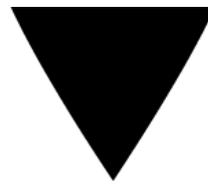
Adherence to Frameworks



NIST 800-53 / VITA SEC 501-09

NIST 800-37 RMF

VITA SEC 520-00 RMF



Industry Momentum

CM and CA have been around for years, but there is currently greater expectation for them to be implemented.



Budgetary Concerns

Agencies have budgetary incentives to take advantage of cost efficiencies from CM and CA.

Following implementation, it should reduce cost of compliance.

NIST 800-37 Risk Management Framework
NIST RMF Task 2-3 - Monitoring Strategy
 Develop a strategy for the continuous monitoring of security posture, changes to the information system and the environment, or operations.
NIST RMF Task 2-4 - Ongoing Security Control Assessments
 Assess a selected subset of the information system and the operations, including personnel and other resources, that are responsible for maintaining the information system to ensure they are performing as intended.

NIST 800-53 / VITA SEC 501-09

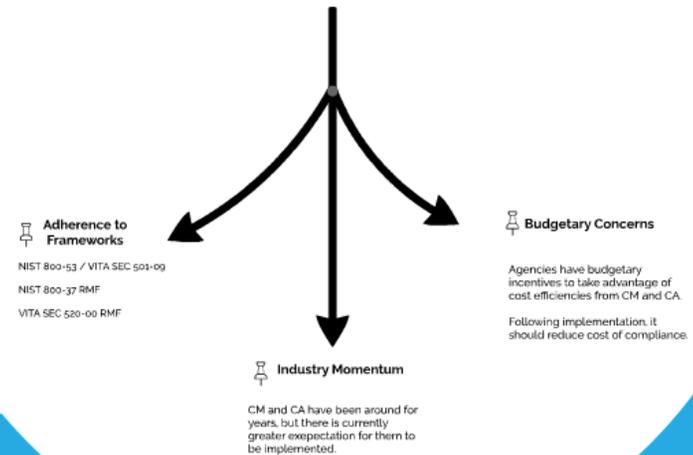
AU-6 Audit Review, Analysis & Reporting

The organization:

- Reviews and analyzes information system audit records at least every 30 days for indications of inappropriate or unusual activity
- Reports findings to designated organizational officials.

Drivers for CM & CA

Adherence to frameworks and industry momentum are driving the search for viable CM and CA solutions.



VITA SEC 520-00 IT Risk Management Standard
 Security Continuous Monitoring (SCM)
 Detect one

VITA SEC 520-00 IT Risk Management Standard

RMF Function

Detect - Develop and implement the appropriate activities to identify the occurrence of an information security event.

The Detect function includes the following categories: Anomalies and Events, Security Continuous Monitoring, and Detection Processes. The function enables timely responses and the potential to limit or contain the impact of potential information security events.

NIST 800-53 / VITA SEC 501-09

AU-6 Audit Review, Analysis & Reporting

The organization:

- Reviews and analyzes information system audit records at least every 30 days for indications of inappropriate or unusual activity
- Reports findings to designated organizational officials.

NIST 800-37 Risk Management Framework

NIST RMF Task 2-3 - *Monitoring Strategy*

Develop a strategy for the continuous monitoring of security control effectiveness and any proposed / actual changes to the information system and its environment of operation

NIST RMF Task 6-2 - *Ongoing Security Control Assessments*

Assess a selected subset of the technical, management and operational security controls employed within and inherited by the information system in accordance with the organization-defined monitoring strategy



VITA SEC 520-00 IT Risk Management Standard

RMF Function

Detect - Develop and implement the appropriate activities to identify the occurrence of an information security event.

The Detect function includes the following categories: Anomalies and Events, Security Continuous Monitoring, and Detection Processes. The function enables timely responses and the potential to limit or contain the impact of potential information security events.

VITA SEC 520-00 IT Risk Management Standard

Security Continuous Monitoring (CM)



DETECT (DE)

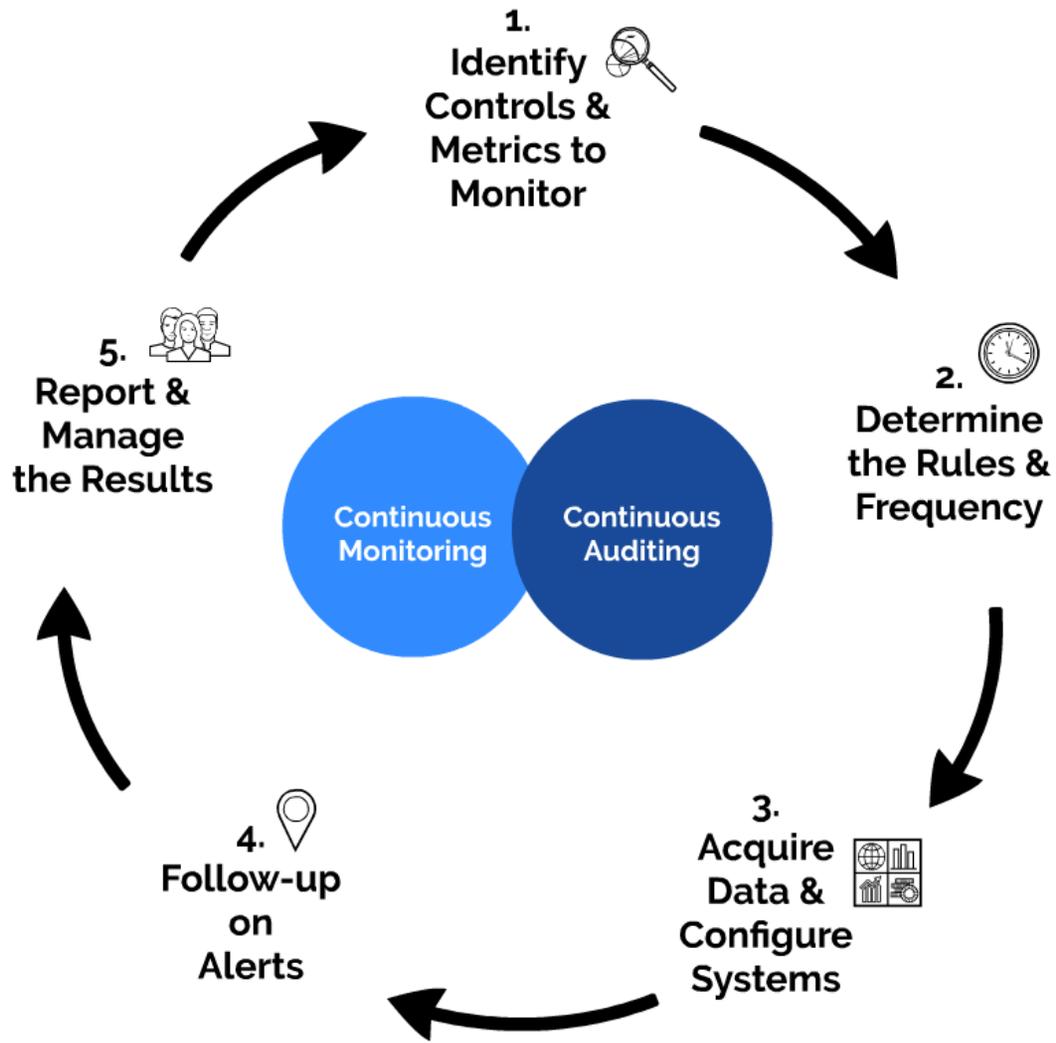


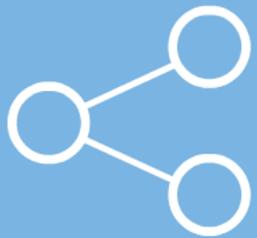


DE.CM - 1:
The network is monitored to detect potential cybersecurity events

DE.CM-4:
Malicious code is detected

**Security
Continuous
Monitoring (CM):**
The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.





Inputs

**Data, Metrics, Internal
Information, Social News**

1.

**Identify
Controls &
Metrics to
Monitor**



2.



Determine the Rules & Frequency

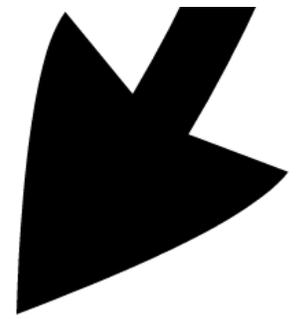
Frequency

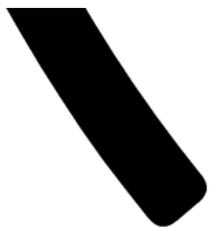
In some definitions, CM and CA does not consist of automated tools. Also includes using manual methods to continuously monitor and continuously audit.

- Includes both automated and manual processes
- Automated tools will usually improve efficiency and cost-effectiveness

Security controls with **higher risk** may be ***assessed more frequently*** than controls associated with lower risk.

3. Acquire Data & Configure Systems

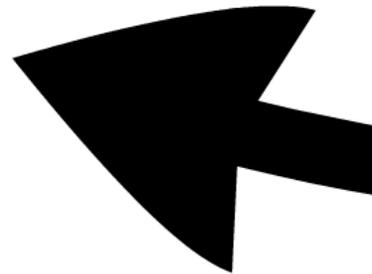




4.



Follow-up on Alerts



5.



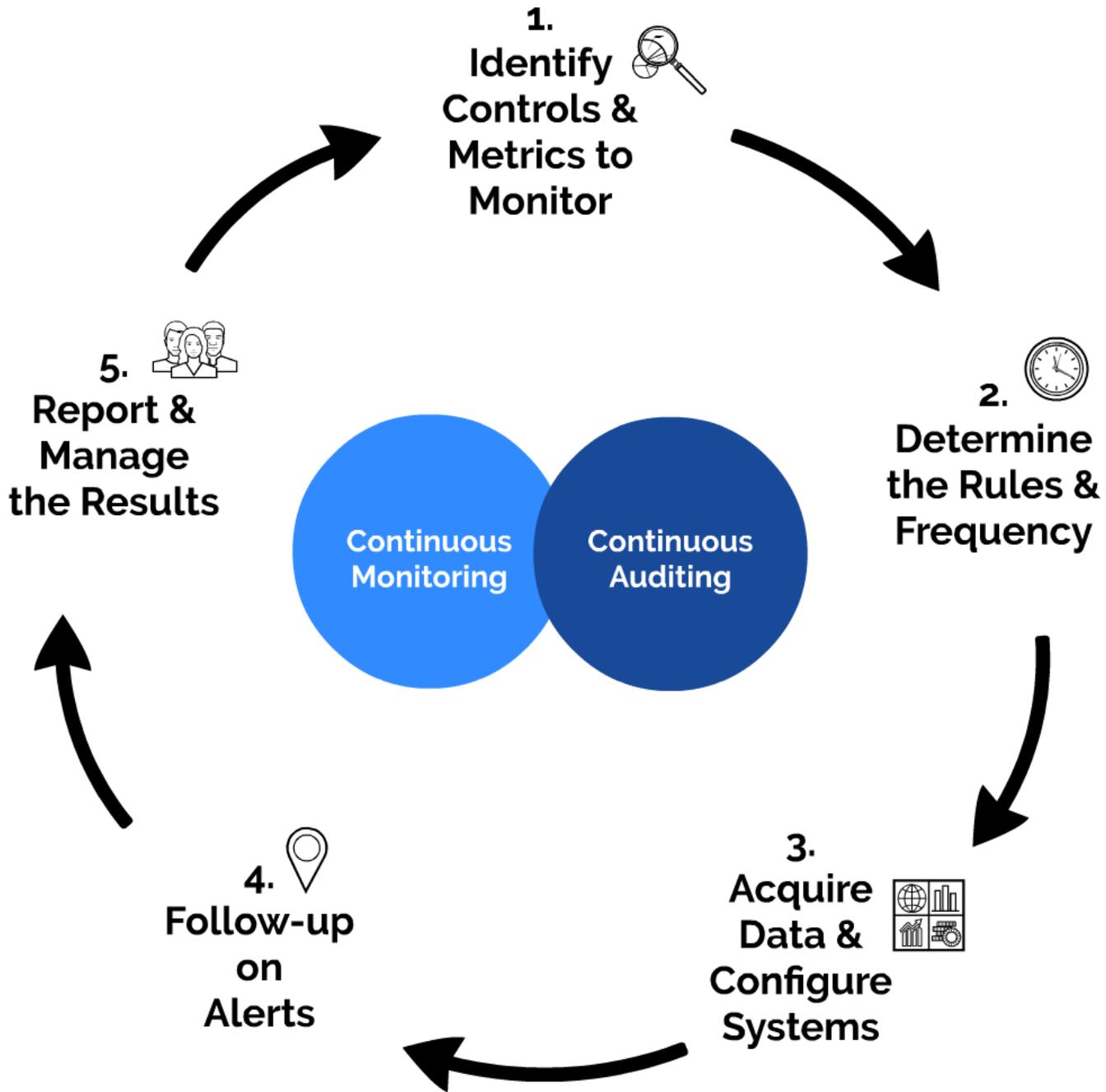
Report & Manage the Results

Continuous Audit Area	2015				2016			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
I	✓	✓	✓	!	✗	✓	✓	!
Approvals	G	G	G	G	Y	G	G	Y
Time Term Access	G	G	G	Y	G	G	G	G
Access Rights Review	G	G	G	Y	R	G	G	R
Successful Logon Attempts	G	G	G	G	G	G	G	G
Management	✓	✓	✓	!	✗	✓	✓	!
Line Configuration	G	G	G	Y	Y	G	G	Y
Change Control	G	Y	G	Y	R	G	G	G



Impacts

**Risk Register, Audit Issues, CAPs /
MAPs, Audit Plan Reporting**

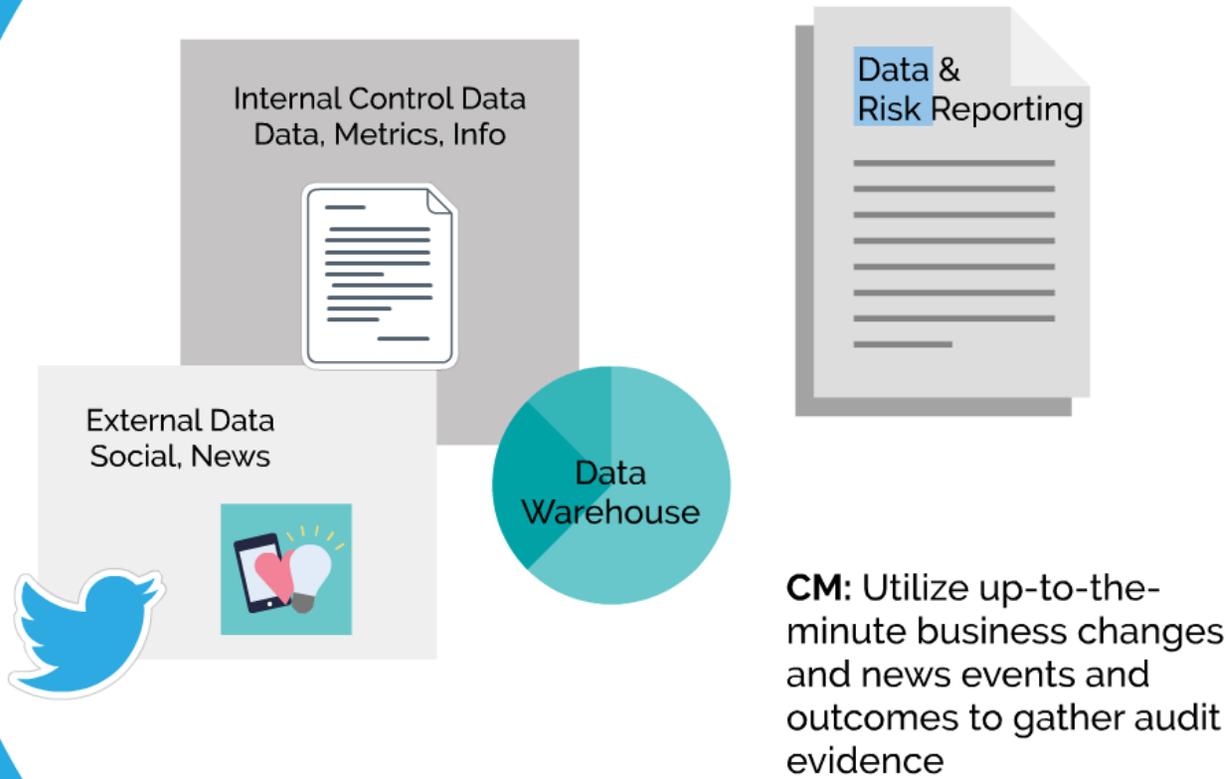


☆ 📊

Risk Register
MAPs, A...

al
ws

CM of key internal and external events and outcomes enables gathering of evidence for CA and / or making real-time adjustments to the audit plan



CM: Utilize up-to-the-minute business changes and news events and outcomes to gather audit evidence

CA: Access exception alert and analyze related evidence to provide on-demand audit opinion

Ac

Co

Benefits to CM & CA

- After initial configuration, there is a time savings and cost savings.
- Consistency of testing procedures from period to period.
- Providing an ongoing evaluation of risks and controls.
 - Increased use of automated security assessments
 - Ability to test more controls and configurations
 - Ability to test higher percentage of population (sometimes 100%)
- Providing timely reporting of gaps and weaknesses, enhancing the opportunity for prompt corrective action.
- Ability to provide more robust reporting to management on the security posture of the organization, key metrics incorporated into regular executive reporting.

Challenges to CM & CA

- Buy-in from Leadership
- Access to data / system access
- Scope of work, determining where to start and place priority
- Programming skills available on team
- Errors in programming, false positives, false negatives (aka missed positives)
- Obtaining the budget / funding for implementation costs

How CM & CA Can Improve Security Posture



External Data
Social, News

Inter
Dat

Benefits to CM & CA

- After initial configuration, there is a time savings and cost savings.
- Consistency of testing procedures from period to period.
- Providing an ongoing evaluation of risks and controls.
 - Increased use of automated security assessments
 - Ability to test more controls and configurations
 - Ability to test higher percentage of population (sometimes 100%)
- Providing timely reporting of gaps and weaknesses, enhancing the opportunity for prompt corrective action.
- Ability to provide more robust reporting to management on the security posture of the organization, key metrics incorporated into regular executive reporting.

Challenges to CM & CA

- Buy-in from
- Access to
- Scope of work where to start
- Programming team
- Errors in positives, false missed positives
- Obtaining for implementation

Challenges to CM & CA

- Buy-in from Leadership
- Access to data / system access
- Scope of work, determining where to start and place priority
- Programming skills available on team
- Errors in programming, false positives, false negatives (aka missed positives)
- Obtaining the budget / funding for implementation costs

Examples of CM & CA

Purchasing

- Late purchase order placement
- Cost increases
- Comparison of vendor addresses to employee addresses

Inventory

- Excess inventory
- Low inventory usage
- Part shortages

Examples of CM & CA

Access Control

- Identify changes to folder security permissions, but not approved
- Identify when additions to privileged groups (e.g., Domain Admins), but not approved
- Identify when User IDs are modified, but access is not approved
- Identify when Employee terms, but access is not disabled timely

Configuration Management

- Identify changes to Configs, but not approved or in-line with baseline security standard

Example Implementation Strategy

Strategy & Planning 3 - 4 months

1. Identify complete population of controls and data
2. Determine the rules & frequency
3. Understand what needs to be tailored to the unique characteristics of your Org
4. Obtain key stakeholder support and strategic direction to set the stage for success down the road



CM & CA Design and Pilot 4-8 months

1. Acquire data
2. Develop a comprehensive framework of automation and process redesign to implement a continuous monitoring program in lieu of traditional
3. Conduct a pilot to test the program design concepts



Implementation 2+ years

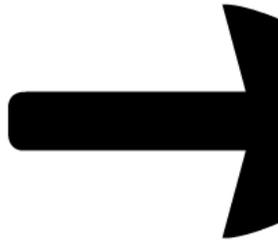
1. Continue to utilize tools and develop automated compliance checks
2. Develop risk reporting database
3. Establish governance processes and change management for program
4. Follow up on alerts
5. Report & manage the results



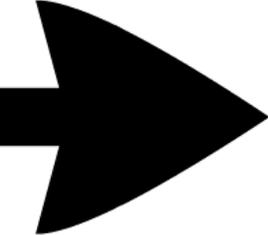
Strategy & Planning

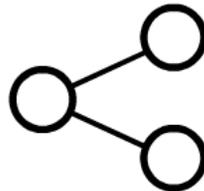
3 - 4 months

1. Identify complete population of controls and data
2. Determine the rules & frequency
3. Understand what needs to be tailored to the unique characteristics of your Org
4. Obtain key stakeholder support and strategic direction to set the stage for success down the road



CM & CA Design and Pilot *4-8 months*

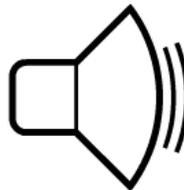
- 
1. Acquire data
 2. Develop a comprehensive framework of automation and process redesign to implement a continuous monitoring program in lieu of traditional
 3. Conduct a pilot to test the program design concepts
- 



Implementation

2+ years

1. Continue to utilize tools and develop automated compliance checks
2. Develop risk reporting database
3. Establish governance processes and change management for program
4. Follow up on alerts
5. Report & manage the results





Lessons Learned

- **Strategy & Planning** - Develop a transition strategy tailored to the agency environment
- **Governance** - Establish policies and procedures to support new processes
- **Change Management** - Deploy training and communications to promote new processes
- **Automation Tools** - Capitalize on existing tools to reduce the cost for automating assessments

Questions?

Ben Sady

Director, *Risk Advisory*

Ben.Sady@dhgllp.com

Peter Tsengas

Senior Consultant, *Risk Advisory*

Peter.Tsengas@dhgllp.com

DHG
DIXON HUGHES GOODMAN LLP

