

2022 Planning and Internal Audit

Universe Considerations

May 2022



Topics

- 01** Identify key factors used for assessing risk
- 02** Describe the risk assessment process and the credit union's payments system universe
- 03** Identify key factors specifically of each product/service for EPS



Polling Question

1

Have you performed your 2022 Risk Assessment?

- a. Yes
- b. No
- c. In process

A close-up photograph of a hand holding a pen, poised to write on a document. A dark chess piece is visible on the right side of the frame. The image is overlaid with a semi-transparent dark rectangle containing the title text.

Key Factors of Risk Assessment



Types of Risk

Systems and Controls

Credit Union management is responsible for establishing an effective risk management system and controls. An effective Electronic Payments Systems (EPS) risk management program includes written policies and procedures, internal controls, and oversight by the Board of Directors to ensure the EPS program is operating within the risk appetite of the Credit Union.

Credit Risk

Credit risk is the risk to the Credit Union's earnings and capital when a customer defaults on a debt or fails to meet the terms of any financial contract. Credit risk arises from all activities where the institution is dependent on the issuer, borrower, or counterparty performance, not just traditional lending activities. For example, a Receiving Depository Financial Institution (RDFI) incurs credit risk if it allows a debit entry to post and overdraw a customer account.

High-Risk Activities

Credit Unions that approve high-risk customers or engage with Third Parties face increased reputation, credit, transaction, and compliance risks.

Risk Assessment Process

Understanding the Business

- Scoping the Assessment
 - Determine organizational structure, product/service offering, customer base and project stakeholders
 - Determine if a “risk appetite” has been established or needs to be established
 - Identify lines of business to identify structure of risk assessment scoping





Risk Assessment Process

Measure and Evaluate Effectiveness of Controls

- Quality of Risk Management
 - Strong quality of risk management indicates that management has effectively identified and controls all major risks posed by the function. The Board and management participate in managing risk and ensuring that appropriate policies and limits exist, and the Board reviews and approves them. Policies and limits are supported by risk monitoring procedures, reports, and management information systems that provide the necessary information and analyses to make timely and appropriate responses to changing conditions. Internal controls and audit procedures are appropriate to the size and activities of the Financial Institution. There are few exceptions identified by Internal Audit to established policies and procedures.
 - Satisfactory quality of risk management indicates that the Financial Institution's internal controls are effective, though could use some improvement. While the Financial Institution may have some internal control deficiencies, these deficiencies have been recognized and are being addressed. Overall, policies, procedures, and limits; risk monitoring processes; reports; and management information systems are considered effective in maintaining a sound control environment.
 - Weak indicates that internal controls are significantly deficient and require greater management and Board attention. The internal control system may be lacking in important respects, particularly as indicated by continued control exceptions or by the failure to adhere to Board-approved policies.

Risk Assessment Process

Evaluate Residual Risk

- Aggregate Residual Risk
 - Aggregate residual risk is the risk derived from assessing the likelihood and impact of risk occurrence after considering management's control activities (quality of risk management). Residual risk is determined to be high, moderate, or low. Typically, the residual risk would be less than the quantity of risk, although occasionally quantity of risk and residual risk may be the same. Three common reasons for this could be:
 - The range of the risk represented in the quantity of risk versus residual risk assessment does not allow for a reduction in the risk rating assigned. For example, something may be at the high end of Moderate for the quantity of risk and be at the low end of Moderate for residual.
 - Existing mitigation strategies are not considered sufficient to reduce the assigned risk level.
 - The impact of a risk event would result in significant exposure to the organization. In spite of well-designed and executed mitigation strategies, no system of controls is fail-safe and able to mitigate all risk events. In situations where even a single control failure will result in significant exposure to the Credit Union, the residual risk will reflect the high impact in spite of well-designed controls structures.

RESIDUAL RISK	Aggregate Inherent Risk		
Effectiveness of Controls	Low	Moderate	High
Strong	Low	Low	Moderate
Satisfactory	Low	Moderate	High
Weak	Low	Moderate	High

Risk Assessment Process

Response

- Develop plan for remediation activities or monitoring risk responses based on output of the Risk Assessment.

Updating

- Annually, if not more frequently are risks changes

Managing

- Develop plan to maintain and sustain the Risk Assessment for future use.

Reporting

- Communicate results to appropriate stakeholders.



Polling Question

2

What is your biggest risk for 2022?

- a. Credit Risk
- b. Compliance Risk
- c. Operational risk
- d. Cybersecurity
- e. Other



Emerging trends, risks and regulatory focus



Overview

Looking ahead through 2022, we continue to see a broad range of uncertainties and challenges, many of which were triggered by the COVID-19 pandemic which remains at the forefront. We have seen digital leaders emerge with their ability to pivot and quickly react to the pandemics new normal while data security and cybersecurity remain ever present in our minds keeping many of our Banks awake at night.

Our role in internal audit requires us to understand key risks and proactively identify emerging risks in order to add maximum value.

As Richard Chambers said - “*In addition, a heightened regulatory environment and dramatic increases in government spending will likely add to the crowded risk portfolios of organizations across all sectors. If internal auditors are to remain risk-centric in the face of new and emerging risks, they will need not only increased resources, but a strong emphasis on agile risk management practices.*”



New, Emerging, or Changing Risks – Technology

Commingling of Cybersecurity and Information Technology

Overview: Responsibilities affiliated with the people, processes, and technologies that encompass Information Technology (IT), Information Security (IS) and Cybersecurity (Cyber) continue to be dispersed across all three lines of an organization – Operations, Risk Management, and Audit. Strong audit practices must continue to reach and collaborate among those responsible for IT, IS, and Cyber.

IA Universe / Risk Assessment Impact: Crowe's Internal Audit methodology is being revised to acknowledge the convergence of IT, IS, and Cyber. In 2022+ we anticipate the IT General Controls Review and the Cybersecurity Assessment will become a single audit. The same auditable units will exist; however, execution, reporting, and documentation will be consolidated into one engagement.



New, Emerging, or Changing Risks – Technology (continued)

Federal Reserve Security and Resiliency Assurance Program

Overview: In October 2020, the Federal Reserve implemented a Security and Resiliency Assurance Program, which includes the requirement for institutions and service providers that utilized FedLine solutions to perform an assessment of their compliance with the Federal Reserve's specific security requirements and submit an attestation that they have completed the assessment. 2021 is the first year of this and the organization's attestation is due by December 31, 2021. Going forward, the attestation will need to be completed once per calendar year (January – December).

IA Universe / Risk Assessment Impact: We are seeing our banks complete these in any of the three lines (Operations [CISO/CIO], Risk [CRO/CISO/ISO], or Audit [CAE]). We should confirm where this is occurring in each organization.



New, Emerging, or Changing Risks – Technology (continued)

SWIFT Customer Security Programme Security Attestations; SWIFT Customer Security Controls Framework

Overview: Similar to the Federal Reserve, SWIFT also has a Customer Security program and an attestation requirement for those organizations with a SWIFT system. This is not a new program, but what is new, is the delineation for review beyond a self-assessment by the users for 2021. An independent assessment can be performed by Risk, Internal Audit or a third party. We have seen some organizations requesting the complete third-party assessment in addition to anything done by the Bank itself. All SWIFT users have to attest before the expiry date of the current controls version, confirming full compliance with the mandatory security controls no later than 31 December, and must re-attest at least annually thereafter.

IA Universe / Risk Assessment Impact: We have observed past years Banks were only completing these primarily through Operations [CISO/CIO]; however, this can no longer be done. Internal audit can perform the assessment and/or a gap analysis leading up to a full / final annual assessment. The Bank would still file the attestation.



New, Emerging, or Changing Risks – Technology (continued)

Targeted Network-based Penetration Testing

Overview: Banks continue to seek new and innovative ways to test and challenge their controls, processes, and employees by performing targeted attacks against their own networks and systems. Historically and still, Crowe executes “penetration tests” for many IA Banks. In order to dig a bit deeper and/or evaluate more specific possible weaknesses, more advanced levels of testing may be valuable to our Banks. These types of tests are referred to as “Red Team”, “Purple Team” and/or “simulation tests”, where we narrow the focus of a test and increase either depth, length of testing, and/or collaboration with those being tested.

IA Universe / Risk Assessment Impact: Examiners continue to expect annual external network-based pentests among financial services and a routine frequency of internal network pentesting – depending on their size and complexity. Even if an organization performs their own internal testing, Internal Audit should (at minimum) perform a validation of scope, conclusion, and management actions. Further, independent and more advanced levels of tests do help organizations further explore, validate, or gain additional insights that bring benefit and more robust audits. These advanced style tests should be considered.



New, Emerging, or Changing Risks – Technology (continued)

Continued Exploration in Robotic Process Automation

Overview: Banks are continuing to deploy Robotic Processing Automation (RPA) [or their vendors are], which drives lower costs and higher efficiency. Areas where banks are investing include: Loan Applications and Servicing, Deposit Account Creation, Account Closure, Customer Service, Know Your Customer (KYC), Quality Assurance (QA) Processing, and Regulatory Monitoring.

IA Universe / Risk Assessment Impact: This area should be a consideration for IA Universe, with starting points on Project Management and lead into specific implementation coverage, which may include validations, exception handling, and change management / development.

Data Governance

Overview: Banks continue to explore meaningful ways to correlate customer data and recognized patterns / trends to drive business decision making, customer targeting, and drive increased revenue. Amassing data, data sharing / selling, and computing outcomes requires increased access controls, monitoring, distinguished roles, and defined data structures.

IA Universe / Risk Assessment Impact: Data Governance should be considered for audit rotations.



New, Emerging, or Changing Risks – Technology (continued)

Sustained Remote Worker Arrangements

Overview: Banks continue to oscillate between on-site, off-site, and hybrid work arrangements. Technology that enables sustained connectivity and access to banking applications have mostly been implemented; yet refinements around usability, security, and access will persist.

IA Universe / Risk Assessment Impact: For Banks who recently added technologies, such as virtual private networks (VPN), virtual desktop infrastructure (VDI), or cloud technologies (Microsoft Azure, Microsoft 365, Amazon AWS,) should consider establishing a routine, risk-based coverage over a three-year cycle.

Business Resiliency

Overview: Adjustments on how employees and systems are accessible and utilized (due to COVID and US Weather Events) drove needed changes in multiple supportive operations and respective documentation, including disaster recovery, business continuity, and third-party risk management.

IA Universe / Risk Assessment Impact: Policies and procedures, including Business Continuity, Incident Response, and Disaster Recovery, have been updated and are continually tested and refined. This area may also be referenced as “resiliency” going forward.



New, Emerging, or Changing Risks – Operational (continued)

Cryptocurrency

Overview: Cryptocurrency adoption continues to trend as Financial Institutions are looking for innovative ways to use this technology to offer additional products/services. Financial Institutions can play a variety of different roles in this space depending on their strategic initiatives and risk appetite. These may include, but not limited to: Providing services through a third-party vendor; Lending fiat against crypto Asset Manager; Depository Institution; Correspondent Bank Custodian.

IA Universe / Risk Assessment Impact: There will probably be little impact to our Banks today. However, the risk assessment process is our opportunity to get involved at the onset of the relationship/initiative. Small, community banks are having these conversations just as much as larger institutions.

Polling Question

3

Have you performed you consider ESG in your 2022 Risk Assessment?

- a. Yes
- b. No
- c. Somewhat
- d. What is ESG?



New, Emerging, or Changing Risks – Operational (continued)

Environmental, Social, and Governance (“ESG”)

Overview: There continues to be ongoing development around Environmental, Social and Governance (ESG) requirements. This is at the forefront of discussions amongst many regulators yet there is currently no finalized regulatory requirements as of today. However, we are starting to see more external pressure for companies to start reporting on ESG. This is coming from investors who want to see more information, but also customers.

IA Universe / Risk Assessment Impact: There is little impact today for our smaller institutions, but for larger or public institutions we should inquire about maturity as it relates to ESG and a formal program to prepare for ESG requirements. We should understand whether the Bank has established a plan for implementing an ESG program, including governance over the reporting of ESG information, selecting an ESG reporting framework, preparing a risk assessment to determine the most important or “material” matters that should be addressed, etc.



New, Emerging, or Changing Risks – Operational (continued)

Board Diversity

Overview: The SEC approved a rule requiring all listed companies to meet certain minimum diversity targets or disclose why they are not doing so. Most Nasdaq-listed companies will be required to have, or explain why they do not have, at least two diverse board members, including one director who self-identifies as female and one director who self-identifies as either an underrepresented minority or lesbian, gay, bisexual, transgender, queer or other (LGBTQ+). Companies with five or fewer board members need to have one diverse board member to meet the target.

IA Universe / Risk Assessment Impact: For any public banks, you should understand how the financial reporting team is preparing for these new requirements to provide statistical information by the later of August 6, 2022, or the filing date of their proxy statement, or information statement for the annual shareholder meeting.



New, Emerging, or Changing Risks – Operational (continued)

Corporate Governance and Strategic Risk

Overview: Strategic Risk is having a greater impact on many of our Banks today. Today's economic environment as a result of the Pandemic has impacted many of our client's growth objectives. Further, the growing need for digital technologies is requiring new skills in the market.

There are many elements that might have a bearing on strategic risk, and talent management can be included within this as more organizations are finding it increasingly difficult to find qualified talent but also managing within a remote workforce. Our Banks will likely face concerns around the pandemic's impact to the labor market. This is further compounded by the effects we are seeing on employee morale and productivity and how these are changing or having an impact on an organizations culture.

IA Universe / Risk Assessment Impact: Strategic Risk is largely considered within a corporate governance audit. We should consider when the last time we assessed our client's corporate governance activities.



New, Emerging, or Changing Risks – Compliance

Fair Lending – Loss Mitigation

Overview: Fair Lending, as a whole, has gained traction with the current social and civil environment, in addition to the current resurgence of the CFPB and other agencies, under the current administration. Additionally, focus is growing on what financial service companies are doing to provide adequate financing and investment opportunities to minority groups and minority geographies.

IA Universe / Risk Assessment Impact: For purpose of Fair Lending, and with the impact of COVID-19 and a loss of jobs, salary decreases, etc., more borrowers will be seeking forbearance, refinances, modifications, and potential foreclosure. Do Banks have an adequate Fair Lending program? Is on-going analysis and monitoring occurring? Are Banks consistently handling underwriting, pricing and loss mitigation regardless of race, gender, ethnicity, marital status, etc.?



New, Emerging, or Changing Risks – Compliance (continued)

Impact of CARES Act / Fair Credit Reporting Act

Overview: The CARES Act requires that consumers whose account was not previously delinquent must be reported as current on their loan if they have received an accommodation and make any payments that the accommodation requires. FCRA requires that information furnishers report accurate information to the credit bureaus. Information furnishing is typically an automated process, where this CARES Act requirement may require financial institutions to manually or systematically alter its information-furnishing practices to be in compliance with the requirement.

IA Universe / Risk Assessment Impact: The scope of the FCRA audit should include a review of operational procedures with regard to reporting of delinquencies. There should also be testing to confirm whether the controls are working effectively, ensuring that late payments and delinquencies are being handled as required under the CARES Act.

Polling Question

4

Has your risk for third-party relationships increased or decreased for your 2022 Risk Assessment?

- a. Increased
- b. Decreased
- c. Stay about the same
- d. Not considered



New, Emerging, or Changing Risks – Compliance (continued)

Third-Party Servicer Relationships and oversight

Overview: Banks are relying heavily on outsourcing of standard banking processes, such as flood, hazard, subsequent Regulation Z and RESPA disclosure requirements, customer service hotlines and more. These activities all consist of heavy regulatory requirements.

IA Universe / Risk Assessment Impact: With reliance on a third party for products and services, confirm oversight of risk management. We are seeing Banks with immature or non-existent monitoring of servicer relationships.

FinTech Partnerships and oversight

Overview: Some Banks are partnering with Fintechs and offering products and services through them.

IA Universe / Risk Assessment Impact: With reliance on a third party for products and services, need to understand processes and oversight. We are seeing fintechs with immature or non-existent compliance functions.



New, Emerging or Changing Risks – Credit Risk

Review of Loan Review and Process

Overview: This has increased in IA plans over the last five years.

IA Universe / Risk Assessment Impact: Loan review functions have become more dynamic, and stakeholders are placing more reliance on the function than ever before. It has become a common and critical look as part of an IA plan and is commonly in an annual or every-other-year regulatory plan.



New, Emerging or Changing Risks – Credit Risk (continued)

Grading Approach

Overview: Many Banks have migrated to new grading processes in the last 10 years (scorecards, matrix, definitions, dual grade, etc.).

IA Universe / Risk Assessment Impact: There have been regulatory publications on less subjective grading scales and regulators have pushed more repeatable grading approaches:

- Limited internal knowledge on how to design a new grading approach
- Lumps in how people implement these and maintain these
- Sometimes are a bit generic at first pass
- Many times, will start the new process but not have fully developed guidelines and procedures
- Sometimes it makes sense to have some IA review after developed

Confirm whether approach for grading commercial loans has changed over the last few years and discuss what tweaks they have done. Have they added scorecards, changed policies, started to use a technology, etc.

Recap

As companies continue to navigate the rapidly changing environment and constant disruptions, we need to search for opportunities to help our Banks add value in how they manage their risks and risk environment.

We must continue to look for opportunities to not only deliver on our audit plan in a challenging environment, but also proactively reach out to Banks to keep them abreast of the challenges they face or which may be coming.

As we have all heard many times from the Greek philosopher Heraclitus, “*The only constant in life is change.*” While our stakeholders are expected to be resilient and have processes ready to respond to change, we as internal auditors, must adapt with them to help them have the controls and solutions in place to be successful.



Third-Party Risk Management

Cloud Vendor Exposure

May 2022

Agenda

01

What is the Cloud?

02

Setting the Stage

03

Updated Regulations

04

Third-Party Risk and the Cloud

05

Cloud Providers in the News

06

Fourth and fifth-party risk

07

We assessed risk – Now what?

08

Q&A/Discussion



Polling Question

1

Does your organization have a formal definition of the “Cloud”?

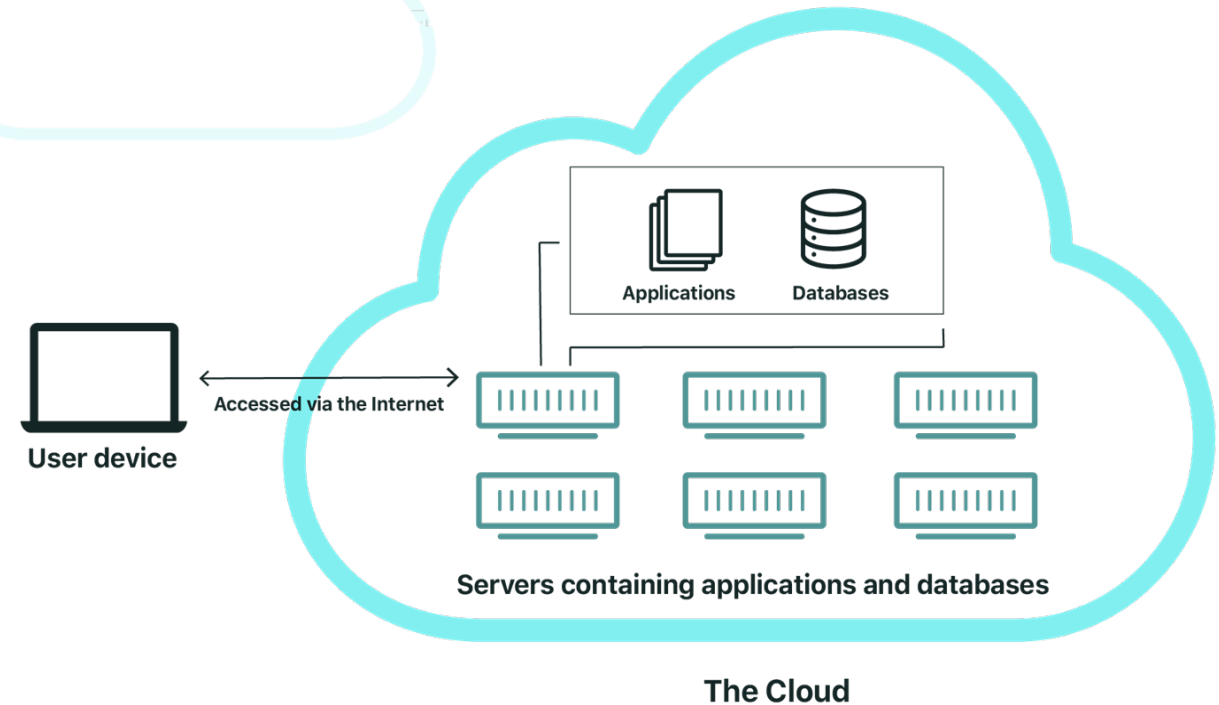
- a) Yes
- b) No
- c) I don't know
- d) There is no cloud. It's just someone else's computer.

What is the Cloud?

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

- The NIST definition of Cloud Computing

<https://csrc.nist.gov/publications/detail/sp/800-145/final>



Cloud Service Models and Examples

Software as a Service (SaaS)

Cloud vendor manages the server and application, client controls only the data

- Salesforce.com
- Office365

Platform as a Service (PaaS)

Cloud vendor manages the server, hosts code for the client. Client manages SDLC

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Compute
- Force.Com

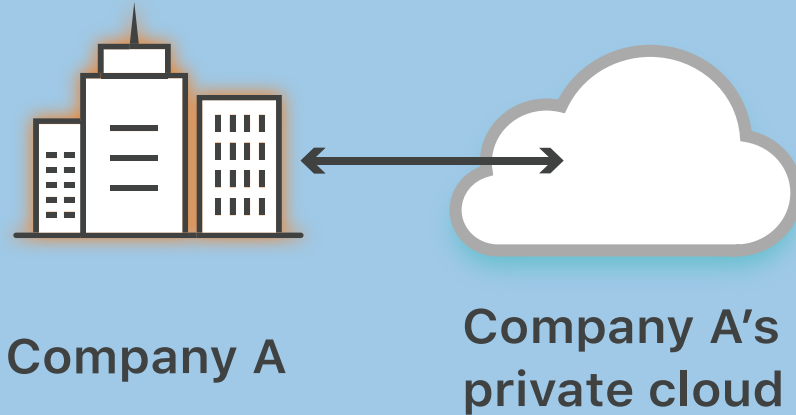
Infrastructure as a Service (IaaS)

Virtualized servers, Cloud vendor manages physical security, some boundary defense, Client controls the rest

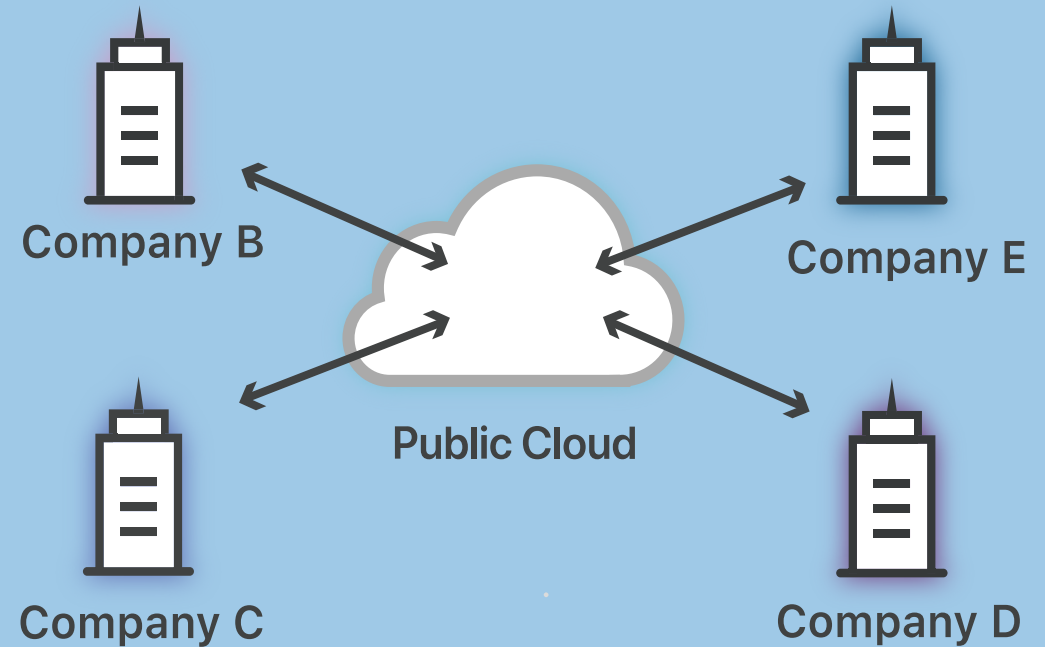
- Amazon Web Services (AWS)
- Microsoft Azure
- Google Compute

Cloud Deployment Models

Private Cloud



Public Cloud (shared by Multiple companies)



<https://www.cloudflare.com/learning/cloud/what-is-a-public-cloud/>

Setting the Stage – Why the Cloud?

- April 2021 study conducted by the Ponemon Institute, found that 46% of IT security professional respondents stated increased efficiency was a reason they were using the cloud, while 45% said reduced cost was a factor.
- This same study found 68% of organizations have a multicloud architecture or strategy, with an average of 4 cloud environments. Of the 32% of respondents who did not have such a strategy, over half said they will have it in 6 months and over a quarter will have it in the next 12.

<https://www.proofpoint.com/us/resources/analyst-reports/cost-of-cloud-compromise-and-shadow-it>





Setting the Stage – So what's the big deal?


- The April 2021 study conducted by the Ponemon Institute found that 72% of IT security professional respondents moving to the cloud has brought new security and compliance risks for their organization.
- This same study again found 67% of the cloud applications deployed at their organizations were deployed by departments other than Corporate IT. These are known as “Shadow IT” applications.
- Only 27% of Corporate Data stored in the cloud is controlled by Corporate IT.

Polling Question

2

Does your organization have a Third-Party Risk Management program?

- a) Yes: and it is in a mature state
- b) Yes: it is not yet mature, but we are working on it
- c) No: we do perform some aspects of TPRM, but we lack a formal program
- d) No: we are not addressing Third-Party risk



OCC Bulletin 2020-46 | April 30, 2020*

Joint Statement on Security in a Cloud Computing Environment

Key Risks Identified Include:

- Cloud strategy alignment
- Appropriate DD and OM
- Contractual Responsibilities
- Cloud Asset Inventory
- Proper Security Configuration, Provisioning, Logging, Monitoring
- Identity and Access Management and Network Controls
- InfoSec and Security Awareness Training
- Data Protection
- Change Management/SDLC
- Business Resiliency and Incident Response

* <https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-46a.pdf>

Third Party Risk and the Cloud

- A strong TPRM program can help identify and mitigate risks related to the cloud:
 - Identification of third parties providing what would be considered “Cloud Computing” technology
 - Documenting material “Fourth Parties”, which may include Cloud Service Providers (CSPs) like AWS, Azure, and GCP
- Performing due diligence during on-boarding, and reperforming that due diligence periodically
- Make sure you are asking the questions
 - Either during Inherent Risk information gathering or directly to the third party as part of your assessment
- Understand the deployment models and the controls the provider should have in place
 - PaaS, IaaS, SaaS
- Request relevant documentation
 - SOC Reports, CAIQs

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Client & end-point protection	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Identity & access management	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Application level controls	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Network controls	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Host infrastructure	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Physical security	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer

Cloud Customer Cloud Provider

Cloud Providers in the News

- On Nov. 26, 2020, Amazon Web Services, the world's largest cloud service provider, experienced a major outage in its US-EAST-1 data center due to a “relatively small addition of capacity” to the Amazon Kinesis real-time data processing service.
- Just over two weeks later, Google's Cloud Platform suffered a major failure in its quota management system, severely reducing the capacity of its authentication system.
- Microsoft Teams went down for around four hours on Monday, alongside Azure and other Microsoft 365 services. Microsoft blamed the issues on “a recent change to an authentication system” took some Microsoft 365 services down. A roll back to the change took longer than Microsoft expected, with the company confirming at 12:35AM ET that “impact has been largely mitigated.”
- Most recently, AWS suffered an outage on 12/7/21. Major US companies were impacted including multiple airlines, Netflix, Venmo, Instacart, and McDonalds.



Fourth- and Fifth-Party Risk Challenges

- Rarely under contract, so your organization has no right to audit or even inquire directly
- Third parties can change their fourth parties without notice, so keeping a full inventory may be impossible.
- Sheer number, so the list of fourth- and fifth-party vendors can stretch into millions of companies
- Heavy reliance on a third party for day-to-day operations

Challenges

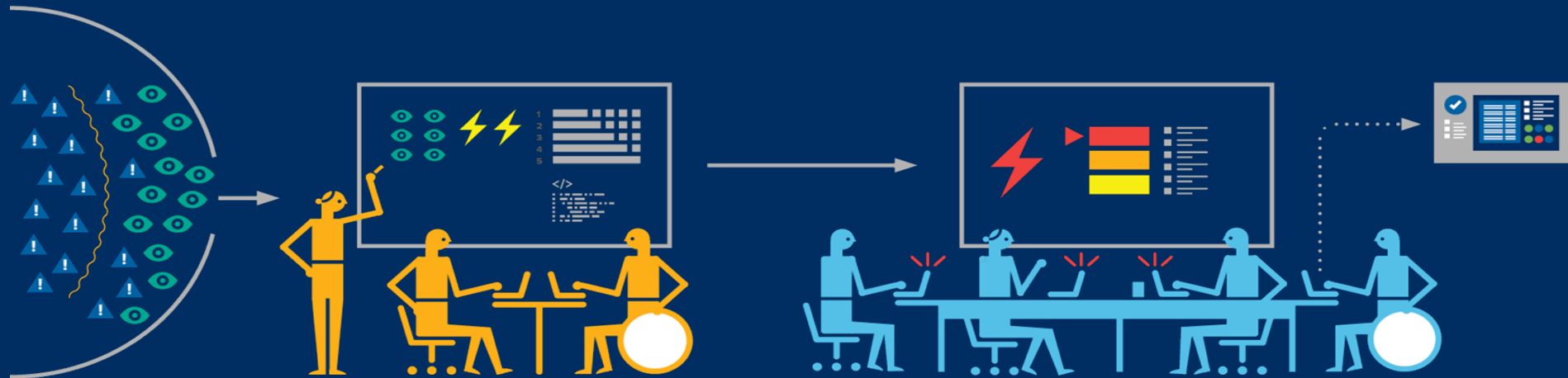
Understanding Fourth- and Fifth-Party Risk

Assess your vendors' third-party risk programs.

- Examine how your vendors' review their third parties
 - Focus on the highest risk areas of the 4th party and verify that those areas are adequately covered by the assessment program.

Only Inventory Key Fourth Parties.

- Not all fourth and fifth parties present equal risk.
- Inventory should include a short list of high-risk, mission-critical fourth parties, which often include Cloud Providers
- Consider use of continuous monitoring platforms to receive alerts



Polling Question

3

Do you have a technology in place to facilitate your TPRM program?

- a) Yes: and we are using it to its full capacity
- b) Yes: but we only have partial buy-in on its use at our organization
- c) No: we are utilizing email/spreadsheets/offline technology to manage
- d) No: we are not managing TPR

We assessed the cloud risk – Now What?

Contracting

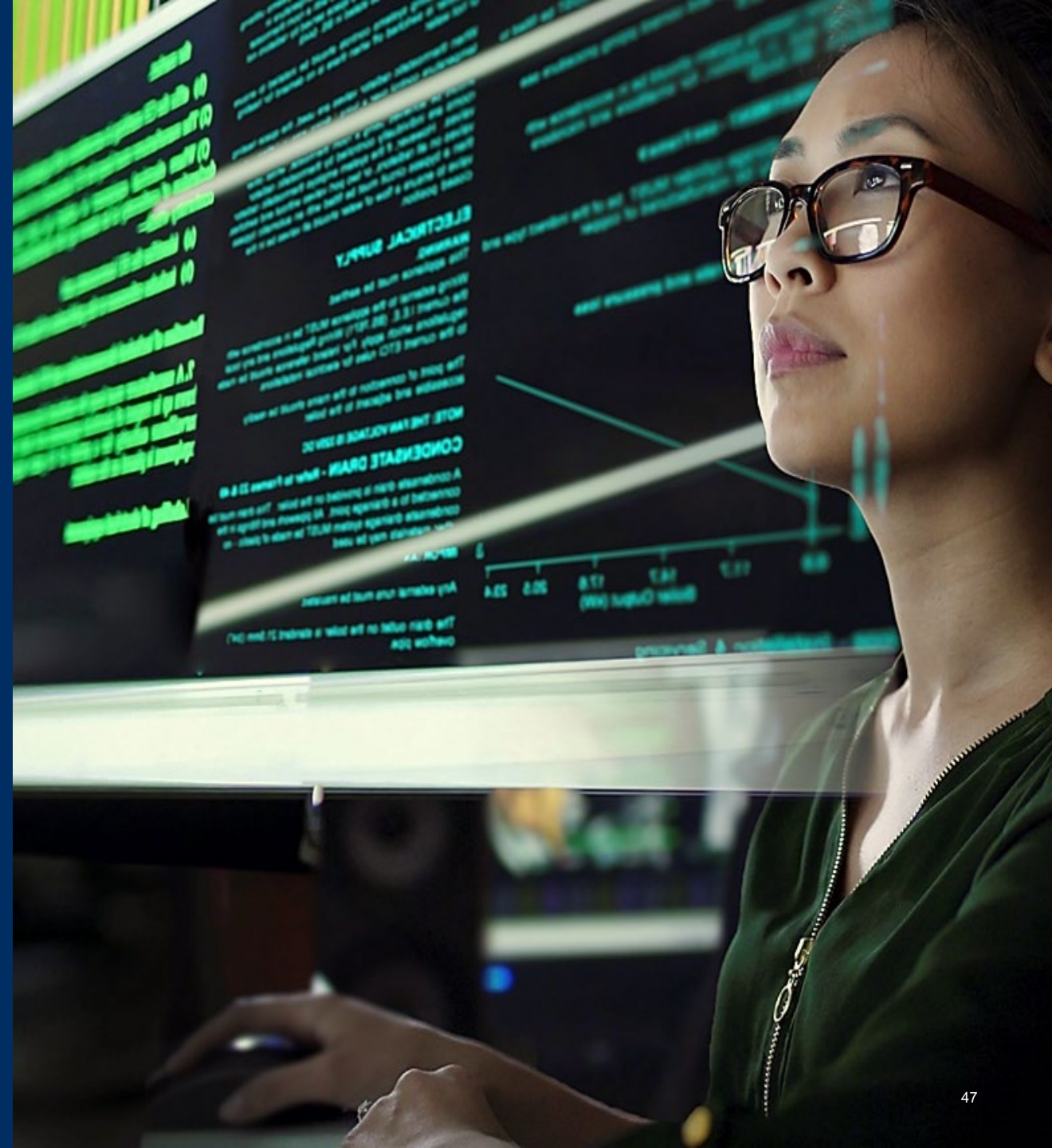
- Understand the involvement of key fourth parties in the delivery of the contract
- Requirement of third party to manage fourth party risks
- Contract clauses



We assessed the cloud risk – Now What?

Ongoing Monitoring

- Reperforming assessments on a periodic basis
- Tracking risks and issues identified to ensure remediation
- Use of continuous monitoring tools to identify vulnerabilities



Polling Question

4

Could your organization provide a report detailing all of its applications that are hosted in the cloud if a report of that type was required today?

- a) Yes
- b) Yes: but we it would require a lot of manual effort
- c) No



Q&A / Discussion



Thank you!



Nate Williams
Nate.Williams@crowe.com
317.208.2472

"Crowe" is the brand name under which the member firms of Crowe Global operate and provide professional services, and those firms together form the Crowe Global network of independent audit, tax, and consulting firms. Crowe may be used to refer to individual firms, to several such firms, or to all firms within the Crowe Global network. The Crowe Horwath Global Risk Consulting entities, Crowe Healthcare Risk Consulting LLC, and our affiliate in Grand Cayman are subsidiaries of Crowe LLP. Crowe LLP is an Indiana limited liability partnership and the U.S member firm of Crowe Global. Services to clients are provided by the individual member firms of Crowe Global, but Crowe Global itself is a Swiss entity that does not provide services to clients. Each member firm is a separate legal entity responsible only for its own acts and omissions and not those of any other Crowe Global network firm or other party. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global. The information in this document is not – and is not intended to be – audit, tax, accounting, advisory, risk, performance, consulting, business, financial, investment, legal, or other professional advice. Some firm services may not be available to attest clients. The information is general in nature, based on existing authorities, and is subject to change. The information is not a substitute for professional advice or services, and you should consult a qualified professional adviser before taking any action based on the information. Crowe is not responsible for any loss incurred by any person who relies on the information discussed in this document. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global. © 2022 Crowe LLP.

The background features a blue-toned image of a robot with its arms raised, overlaid with various digital and data-related graphics. These include hexagonal patterns, binary code (0s and 1s), and abstract light effects. A semi-transparent dark blue rectangle is positioned behind the main title text.

Robotic Process Automation (RPA)

Layne McGuire
May 2022

Polling Question

1

Have you worked with RPA?

A.) Yes

B.) No

C.) I might have but I don't know what it is


Polling Question

2

Are you aware of any business units in your organization that have implemented RPA for any processes?

- A.) Yes
- B.) No
- C.) I might have but I don't know what it is

What is Robotic Process Automation (RPA) and where is it applicable?

- 
- Advanced software designed as robots to mimic human actions
 - Non-intrusive & interacts with existing UI
 - High frequency, deterministic & rules-based processes
 - High Volume
 - Digital Assistants

Hand Work

Polling Question

3

What % of the workflow do you think can be automated?

A.) 45%

B.) 65%

C.) 35%

D.) 95%



Why is RPA Important?

- It is estimated that 45% of workforce tasks can be automated.
- This could save an estimated \$2 trillion in global workforce costs.
- Low-cost and easy to implement.
- RPA can significantly reduce and in some cases eliminate the need for human intervention in performing low-value, mandatory audit testing.
- By allowing internal audit professionals to spend even more time on strategic activities, advanced RPA can promote greater collaboration among the three lines of defense, with the ultimate goal of enabling an integrated approach to risk management.

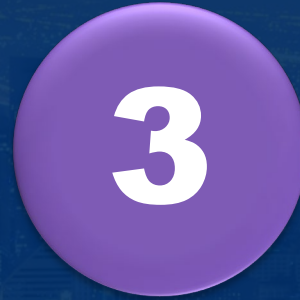
4 Examples of RPA in the World Today



Invoice
Processing



Hiring
and Onboarding



Inventory
Management

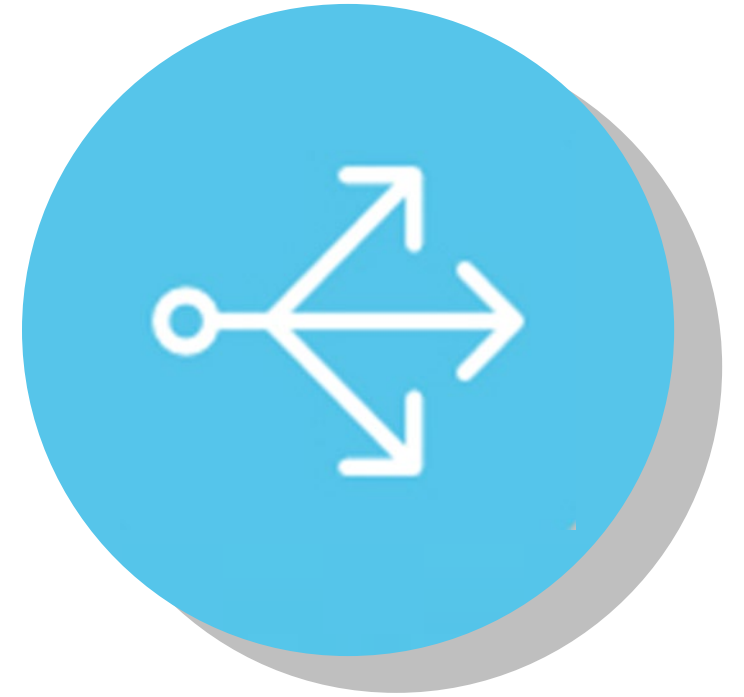


Payroll

RPA in Internal Audit

Key Risks to Understand Prior to the Implementation of RPA:

- Operational
- Financial
- Organizational
- Strategic
- Regulatory
- Technology and Cyber
- Artificial Intelligence

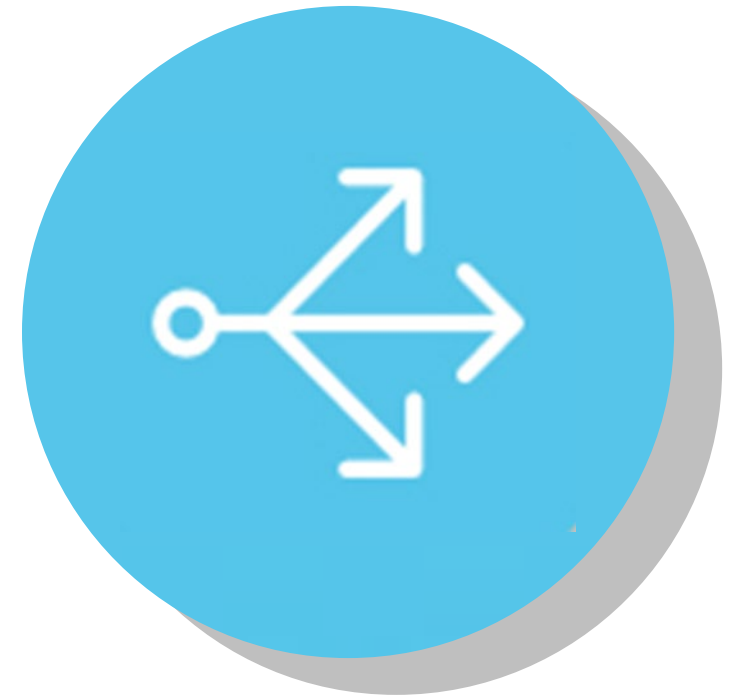


Internal Audit
Risks

RPA in Internal Audit

RPA Implementation:

- Define and Design
 - A project's scope, requirements, budget, timeline and approach should be clearly defined.
- Build and Refine
 - The implementation team develops the complete product in potentially deployable increments and increases efficiency through frequent feedback and improvement cycles.
- Test and Deploy
 - The product or solution is mature enough to be deployed to the end-user domain.

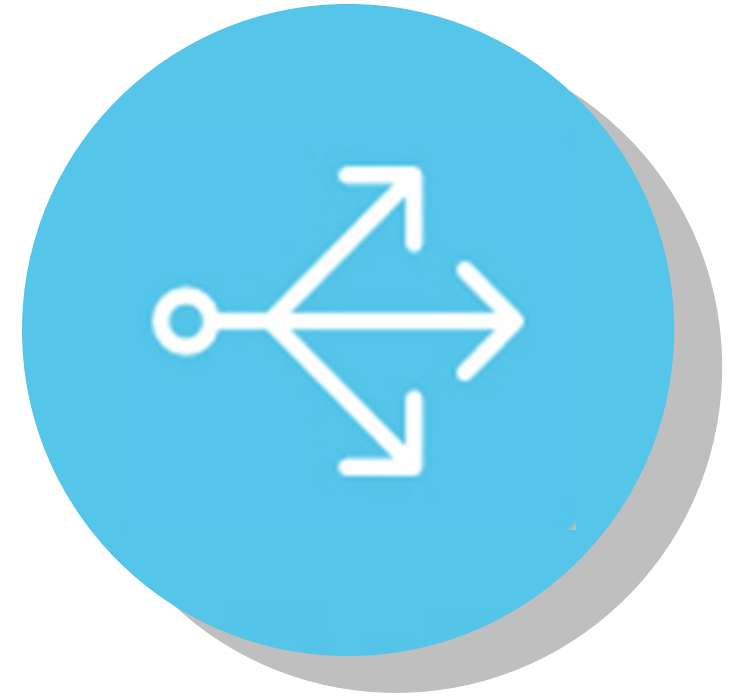


Internal Audit Implementation

RPA in Internal Audit

Key Considerations During RPA Implementation

- During RPA implementation, securing accounts provisioned for bots, segregating duties, password management governance and access attestations are critical.
- Automation continuity planning becomes needed as human dependency on automated work steps increases.
- Testing strategies need to consider data quality, upstream/downstream dependencies on systems and human actions.
- The ability for non-technicians to develop automations creates a need for governance of development activities, release management and coding standards.
- The governance structure needs to consider both the scaling approach and the risk control management of automation.
- Generic bot identification often poses risk of noncompliance to software licenses due to potential indirect usage.



Internal Audit Considerations

How Can RPA Be Applied to Internal Control



What Are the Impacts to Internal Audit?

RPA as a Service

1

Need to understand the technology

2

Opportunity to influence control design & governance

3

Potential to increase audit efficiency

4

Free up capacity to focus on higher priorities

5

Need to develop new testing approaches

6

Consider need for changes to IA staffing model

Polling Question

4

Which of the following is not an Impact of RPA to Internal Audit?

- A.) Potential to increase audit efficiency
- B.) Need to develop new testing approaches
- C.) Consider need for changes to IA staffing model
- D.) These are all Impacts of RPA to Internal Audit

RPA in Internal Audit



Assessment Stage



Fieldwork Stage

- RPA can be configured to identify and respond to potential fraud such as money laundering using automated rules-based monitoring of transactions (e.g., flagging activities for auditors' review), which helps auditors focus on other risk areas.
- RPA can help detect suspicious logs associated with IT systems. Gathering audit documentation/evidence is a semi-manual process that is time consuming and very detail-oriented. Automatically gathering documentation of business processes and IT systems, transactions and controls helps provide continuous assurance, thereby enabling quicker corrective action.
- One particular set of US Sarbanes-Oxley Act (SOX) controls testing relates to user access of systems. The prescribed test plan has historically been largely manual and must be executed quarterly. Automation through RPA augments existing manual effort by relieving strain on human resources.



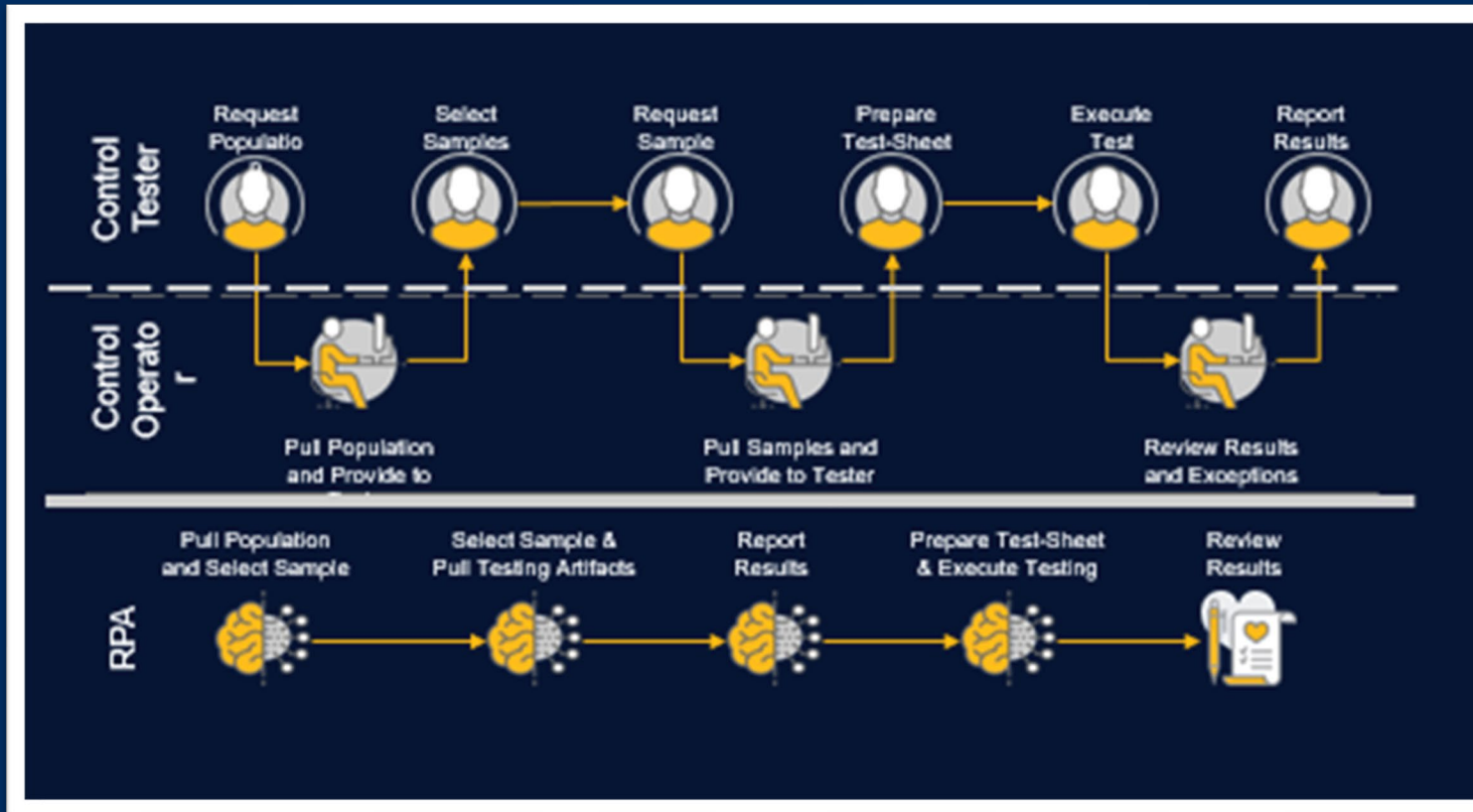
Closing and Follow-up

Sample RPA Use Cases

- Internal Control/Repetitive Operational Audits
 - Request lists
 - Sample selection
 - Status trackers
 - Deficiency logs
 - Exit Meeting Agenda
- Areas Digital Assistant can support Testing:
 - Logical Access/Change Management/Computer Operations
 - Repetitive areas in Business Controls, including but not limited to
 - Account Reconciliation
 - Three-way matching
 - Re-calculation
- Corporate Governance (framework, process and policy review)
- Continuous Monitoring (transaction monitoring/breach of privileges)
- Information Technology/Application Controls (SOD/Least Privileged Access)

How does the User Access Review (UAR) “bot” work?

A high-level view of how a “bot” typically operates





Sources

- <https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/robotic-process-automation-internal-audit.html>
- <https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/robotic-process-automation-for-internal-audit>
- <https://www2.deloitte.com/us/en/pages/risk/articles/internal-audit-robotic-process-automation-adoption.html>
- <https://www2.deloitte.com/us/en/pages/advisory/articles/moving-internal-audit-into-robotic-process-automation.html>
- <https://www.thoughtfulautomation.com/blog/5-real-world-rpa-examples-that-save-time-and-money>



Thank you!

"Crowe" is the brand name under which the member firms of Crowe Global operate and provide professional services, and those firms together form the Crowe Global network of independent audit, tax, and consulting firms. Crowe may be used to refer to individual firms, to several such firms, or to all firms within the Crowe Global network. The Crowe Horwath Global Risk Consulting entities, Crowe Healthcare Risk Consulting LLC, and our affiliate in Grand Cayman are subsidiaries of Crowe LLP. Crowe LLP is an Indiana limited liability partnership and the U.S member firm of Crowe Global. Services to clients are provided by the individual member firms of Crowe Global, but Crowe Global itself is a Swiss entity that does not provide services to clients. Each member firm is a separate legal entity responsible only for its own acts and omissions and not those of any other Crowe Global network firm or other party. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global. The information in this document is not – and is not intended to be – audit, tax, accounting, advisory, risk, performance, consulting, business, financial, investment, legal, or other professional advice. Some firm services may not be available to attest clients. The information is general in nature, based on existing authorities, and is subject to change. The information is not a substitute for professional advice or services, and you should consult a qualified professional adviser before taking any action based on the information. Crowe is not responsible for any loss incurred by any person who relies on the information discussed in this document. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global. © 2022 Crowe LLP.

Compliance Trends

May 2022

Topics

- 01** Regulatory Update
- 02** Consumer Compliance
- 03** BSA/AML



Polling Question

1

What do you expect to be the biggest regulatory compliance challenge for your institution during 2022?

- A. BSA/AML compliance
- B. Consumer compliance/Fair Lending
- C. Environmental financial risk management
- D. Third party risk management
- E. Other / don't know

Regulatory Update



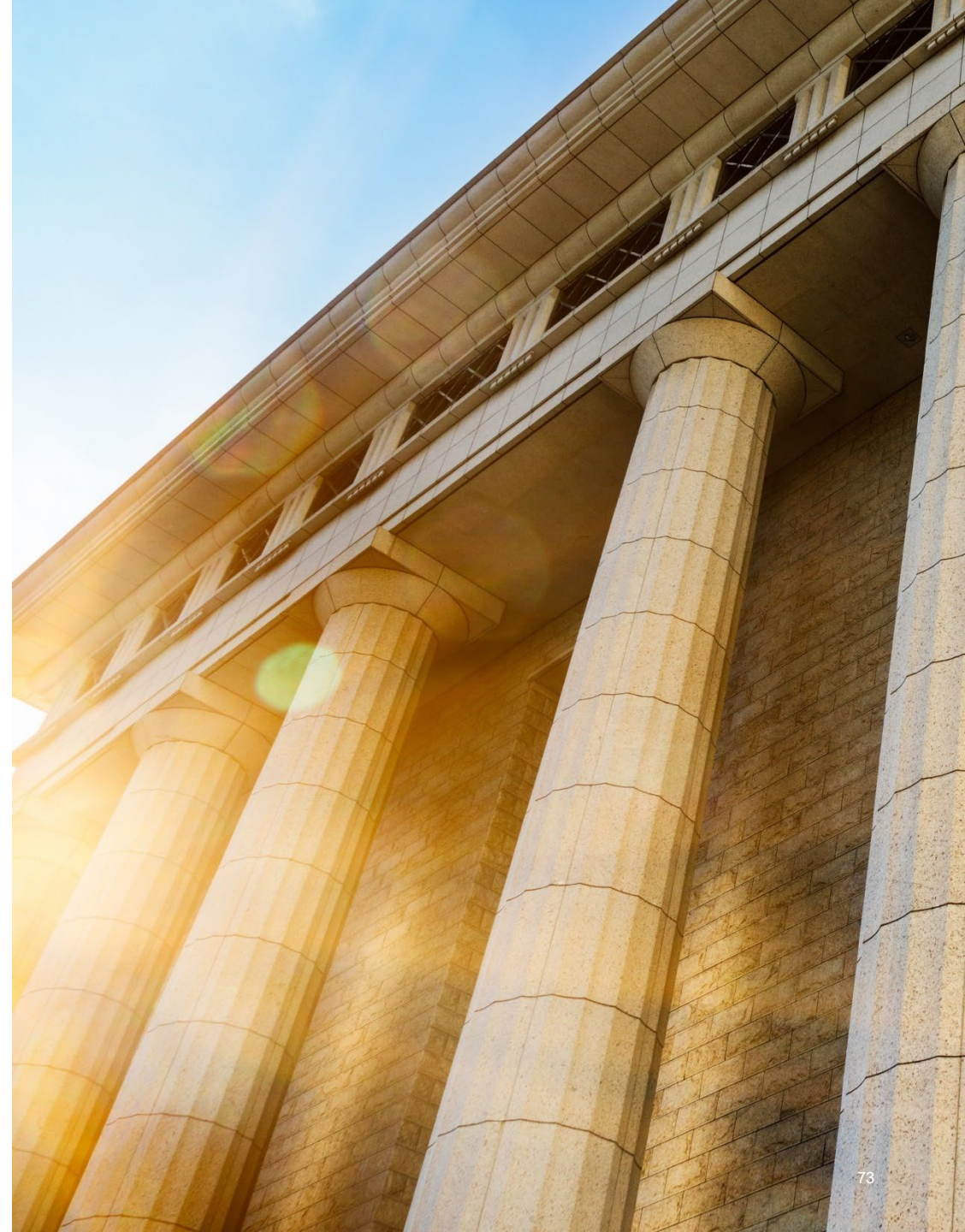
Regulatory Leadership

Awaiting confirmation of new agency leaders

- CFPB: Rohit Chopra
- OCC: Michael Hsu (acting)
- FDIC: Martin Gruenberg (acting)
- NCUA: Todd Harper
- FinCEN: Him Das (acting)

Expect an accelerated pace of regulatory change

- Refined approaches to supervision
- Shift from pandemic relief efforts
- Resuming on-site examinations



Consumer Compliance

CREATIVITY
CONCEPT
RELIABILITY
LOYALTY
EVALUATION
GOAL
ASSESSMENT
ANALYSIS
MOTIVATION
STRATEGY
COMPETENCE
RESULTS
VISION
COMPLIANCE
ACHIEVEMENT
PERFECTION
QUALITY
EXCELLENCE

Regulatory Focus

- Regulators will continue to examine for compliance with applicable consumer financial protection laws and regulations. Sharpened focus will occur in the following areas:
 - Fair Lending
 - Redlining/market penetration
 - HMDA Data Accuracy
 - Loan Servicing
 - Credit Reporting Accuracy
 - Deposit Compliance
 - Regulation E Error Disputes (
 - Overdraft Programs
 - Other



Do you know what your data will reflect?



Fair Lending Update: Current Environment

- Lender Concerns
 - Regulatory Priorities – Where are they headed
 - Insufficient understanding of the institutions data
 - HMDA Data Accuracy
 - Redlining and Market Penetration
 - Lack of resources

Fair Lending



Fair Lending Update: Current Focus

Fair Lending has gained significant traction with the current social and civil environment and the resurgence of the CFPB and the other agencies.

- What does this mean?
- Expectation of a ramp up of enforcement orders and Pronouncements
- CFPB to have a larger impact on fair lending expectations
- A review of fair lending risks within PPP Portfolio
- Proposed expanding data collections to include small business lending (comment period ended in January 2022)

Fair Lending



CFPB proposes to require banks to collect and report data on small-business loans

- Like collection of HMDA data – would include race, sex, and ethnicity of the principal business owners, as well as which applicants are denied
- Threshold for reporting is 25 or greater small business loans originated in a year
- An overarching concern is that the new data will be used for supervision and enforcement
- Industry concerned the regime will lead to more fair lending enforcement and public shaming of banks for alleged discrimination against minority-owned businesses
- Bankers also say the rule will be costly to implement and painful; questioning the lack of clarity about what the law and regulatory doctrine is around fair lending to small businesses
- Community advocacy groups are already planning to use the data to publicize which banks are doing a poor job of lending to Black- and Hispanic-owned small businesses
- Comes against the backdrop of banks and fintechs making nearly \$800 billion in small-business loans during the pandemic



New Priorities

- Renewed focus under new administration. When combined with rising pressure to address racial and social injustices and increased data accessibility, fair lending risk is greatly heightened for all financial institutions
- CFPB included various aspects of Fair Lending in the Supervisory Highlights, Fall 2021 edition (https://files.consumerfinance.gov/f/documents/cfpb_supervisory-highlights_issue-25_2021-12.pdf)

Some Key Themes from Supervisory Highlights

- Data analysis –Regulators today don't even need to enter your institution to find a violation. Does your institution know what's in the data? Small business data collection may be on the horizon
- Redlining and majority minority census tract penetration –must focus on marketing efforts
- Many issues observed related to HMDA accuracy –honeymoon period (from 2018) is over
- Pricing discrimination in the granting of pricing exceptions based on competitive offers with policies not appropriately addressing
- Religious Discrimination with lenders asking specific inquiries about religion



Trustmark National Bank Enforcement Action

October 2021

- DOJ and CFPB allege that Trustmark “engaged in a pattern or practice of unlawful redlining” in Memphis, TN
- The Bank “discriminated against Black and Hispanic borrowers and discouraged prospective minority applicants from applying for home loans”
- “Only 4 of its 25 full-service branches were located in census tracts that were made up of mostly Black or Hispanic residents, though half of the census tracts in Memphis are majority minority”
- The bank also avoided locating branches or hiring loan officers in minority communities

Trustmark must:

- Open a loan office in a Memphis neighborhood with a majority of Black and Hispanic residents
- Devote \$400,000 to development partnerships
- Spend at least \$200,000 a year to advertising outreach and credit repair initiatives in Memphis
- Pay a \$5 million Penalty and \$3.85 Million to increase access in neighborhoods impacted by redlining

Attorney General Comments

- U.S. Attorney General Merrick Garland said that the DOJ will combat redlining through a new partnership between its civil rights division and U.S. attorneys' officers, which will work in coordination with the CFPB
- Garland stated that the homeownership gap between minority groups and whites is wider today than in the 1960s: Whites: 74% compared to 49% for Hispanics and 45% for Blacks, according to the U.S. Census Bureau



Some Specific Quotes from Attorney General Garland's news conference on October 22, 2021:

- “Redlining remains a persistent form of discrimination that harms minority communities”
- “The civil rights division has several redlining investigations pending and plans to open more in the months ahead”
- “We are wasting no time getting to work”
- “You can expect more cases like the one you’re seeing today”

“At this news conference, the DoJ stated they are teaming up with the CFPB and the OCC to launch the most aggressive effort yet to combat mortgage lending discrimination”

Elements of an Effective Fair Lending Program

Comprehensive Program

- Board and Executive Management Oversight
- Fair Lending Strategy
- Policies and Procedures (“Program”)
- Enterprise-wide Implementation
- Coverage in all Three Lines of Defense

Competent Day-to-Day Program Management

- Fair Lending Officer
- Fair Lending Committee (Board and/or Management)

Data Collection and Analysis

- Coverage of all lending portfolios, not just residential
- Small business loans portfolios will be a focus going forward

Management and Board Reporting

- Ensure appropriate levels are seeing data

Training – Boardroom to Basement

- Meaningful and targeted





Basic Expectations and Risk Exposure

The Basics

- That all prospective applicants for credit receive fair and equal treatment
- Programs in place to prevent overt discrimination, as well as:
- Disparate Impact and Disparate Treatment
- Predatory Lending
- Unfair and Deceptive Practices

Risk Exposure and Sources of Risk

- Inadequate Fair Lending Programs
- Market Strategy that doesn't take fair lending into consideration
- Lending Discretion – What can lenders can do on their own presents risk
- Lending Exceptions – Inconsistency among borrowers; failure to monitor for issues
- Third Parties – How reliable and effective is their Fair Lending Risk Management Processes?



Lines of Defense

- The 1st Line of Defense must play a key role in fair lending compliance
- 2nd line doesn't DO fair lending; it oversees activities and serves as subject matter expert to the business lines
- The 1st Line should be focused on:
 - Consistent and effective monitoring of fair lending risk
 - Mitigation of risk and execution controls
 - Job-based training expectations of regulators
- The 2nd line must have a proactive fair lending and UDAAP program
 - Issues tracking, monitoring (data analysis and trending) – it's not enough to only be reactive
 - Risk assessment, actionable reporting
- The 3rd line must provide independent, objective assessment of whether the fair lending compliance management system and risk culture is operating as management, the Board of Directors, and regulators expect.



Regulatory Focus

Headlines over the last three months have shed light on this current focal point by the regulators. Have you considered the ramifications of remaining status quo?

Overdraft Programs

- Consider fee amounts and limits, including a de minimis amount and daily limit. Are you in line with your geographic peers?
- Consider a certain account that has overdraft privilege
- Monitoring of complaints to be proactive
- Monitoring of returned fees for disparate impact/treatment

Key Themes

- Ongoing UDAAP concerns
- Unclear processes and customer communication around multiple overdraft programs – general overdraft protection program and Reg E opt-in for POS/ATM
- Technical items, such as charging multiple overdraft fees when ACH transactions are resubmitted
- Institutions moving away from overdraft fees

Polling Question

2

Has your institution eliminated its overdraft fee

- A. Yes
- B. No, and no plans to
- C. Currently under review
- D. Other / don't know



Regulatory Focus

Regulation E Error Disputes

- CFPB issued updated FAQ documents in June 2021(<https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/>)
- Also included various aspects of the Reg E error resolution process in the Supervisory Highlights, Summer 2021 edition(https://files.consumerfinance.gov/f/documents/cfpb_supervisory-highlights_issue-24_2021-06.pdf)

Key Themes

- Issues with Provisional Credits
- Failure to conduct reasonable/timely investigations
- Failure to properly remediate errors (crediting interest and fees)
- Coercion to file police reports and requiring written confirmation of the error

Regulatory Focus



Regulatory Focus

Fair Credit Reporting Act

- Did we handle our members data according to the CARES Act requirements?
- When the dust settles from the last couple years, are we confident that have been reporting timely and accurately?
- Have we tested the integrity of our Metro 2 reporting?
- Are we monitoring complaints for FCRA related complaints?
- Is our dispute process handled centrally or is it decentralized and are we confident it is handled consistently? (i.e., Operational procedures and guidance in the first line)

Key Themes

- Processes to confirm accuracy of credit reporting information, especially changes due to loss mitigation programs
- Reporting accuracy under CARES Act
- Review of credit report disputes

Regulatory Focus



Regulatory Focus

What else should we be thinking about?

- Community Reinvestment Act
- Servicemembers Civil Relief Act
- Debt Servicing
- UDAAP related risk across the enterprise
- Monitoring of Vendors (overdraft vendors, mortgage sub-servicers, flood vendors)
- Relationships with fintechs (are we confident in their Compliance Program, models, complaint management?)

Regulatory Focus

Polling Question

3

If you had a little extra time and a little extra budget, where would you spend it?

- A. BSA/AML compliance
- B. Fair Lending Program and Data Analysis
- C. Complaint Management software
- D. Compliance risk assessment and Program development
- E. A party for my team
- F. Other / don't know

Bank Secrecy Act – Anti Money Laundering



Polling Question

4

What is your biggest concern regarding your BSA/AML Program

- A. Tools in place are inadequate
- B. Limited staffing resources
- C. Changes in regulations
- D. Sanctions Program

AML Act of 2020



- Passed on January 1, 2021, the FY2021 National Defense Authorization Act (“NDAA”) includes some of the largest revisions to the Bank Secrecy Act (“BSA”) and other Anti-Money Laundering (“AML”) regulations since 2001.
- Comprised of 4,500 pages of which approximately 200 pages are specifically related to AML/BSA reform and Countering the Financing of Terrorism (“CFT”).
- There are five key sections we will cover today relating to BSA/AML regulations, which may impact an organization’s compliance efforts.

The five sections of the NDAA related to BSA/AML reform include:

- 1) Strengthening Treasury Financial Intelligence, AML, and CFT Programs;
- 2) Modernizing the AML and CFT System;
- 3) Improving AML and CFT Communications, Oversight and Processes;
- 4) Establishing Beneficial Ownership (“BO”) Information Reporting Requirements; and
- 5) Miscellaneous.



See additional details
in Appendix.

AML Act of 2020

The AML Act of 2020 generally addresses two primary objectives:

Objective #1:

Increasing BSA/AML Effectiveness and Modernization

- ✓ US Government maintained Beneficial Ownership Registry
- ✓ AML Enforcement Priorities Publication
- ✓ Increased collaboration with the public and private sectors
- ✓ Sharing of SARs with foreign branches and affiliates
- ✓ Review of CTR and SAR thresholds as well as streamlining of processes

Objective #2:

Increasing BSA/AML Enforcement Authority and FinCEN Responsibilities

- ✓ Enhanced Subpoena Authority for foreign bank records
- ✓ Expanded BSA AML Penalties and provisions for whistleblowers

Impact of Covid-19



The effects of COVID-19 on AML Programs

Suspicious Activity Monitoring

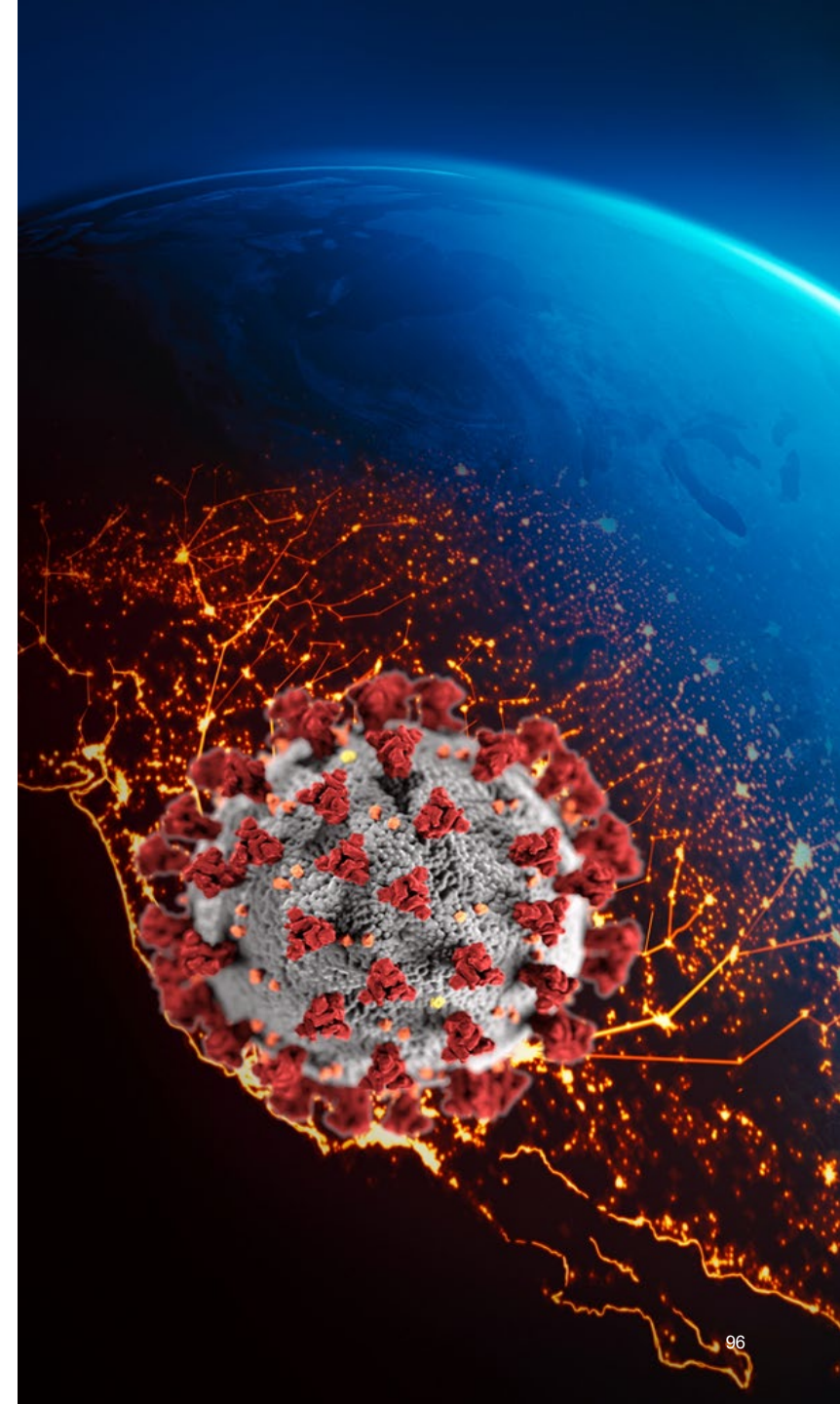
- Discussions with our client partners has revealed an overall decline in alert and case volumes as people are spending less money.
- Renewal of “normal” market activity expected to bring increase in alert volumes.
- FI’s which utilize historical average TM rules expected to see largest discrepancies.

Due Diligence Programs

- CDD and EDD reviews needed to consider new behaviors which may have occurred during social distancing mandates.
- May include individuals and businesses seeking supplementary revenue, one-off large purchases and income decreases.

Fraud Increase

- FIs were at risk of heightened levels of fraud as individuals attempt to exploit the COVID-19 pandemic.
- The Coronavirus Act, Relief, and Economic Security Act (CARES Act) present opportunities for fraudsters.



FinCEN Explains Significant Impact of BSA Data on Law Enforcement Efforts

COVID-19 FRAUD: Federal Bureau of Investigation

- FBI and the SBA Office of Inspector General initiated an investigation into submission on behalf of five (5) businesses of fraudulent PPP loan applications for approx. \$800,000 each.
 - Authorities seized a vehicle valued at \$125,000, jewelry, over \$120,000 in cash, and over \$3 million from 10 bank accounts.
 - Defendants were charged with:
 - Conspiracy to Commit Bank Fraud,
 - Wire Fraud,
 - False Statements to a FI, and
 - Money Laundering.



A network of glowing blue nodes connected by lines, set against a dark blue background with a subtle globe and star pattern. A semi-transparent grey rectangle is positioned behind the word 'Sanctions'.

Sanctions



Russia Sanctions Update

OFAC leveraged Executive Order 14024, dated 4/19/21, to impose additional and complex sanctions to deal with the conflict in Ukraine: these include:

- Specially Designated National (SDNs) – Targeting specific individuals or entities for which transactions must be blocked and assets must be frozen.
- Sectoral Sanctions (SSIs) – Targeting specific sectors of the Russian economy as well as transactions to/from the “covered regions” - Donetsk People's Republic (DNR) and Luhansk People's Republic (LNR).
- Menu-Based Sanctions (NS-MBS) – Targeting individuals or entities with other sanctions/restrictions.

Risk Management Implications:

- Re-assessment of OFAC risk
- Lists used for OFAC interdiction software:
 - Daily updates of lists used
 - Addition of major cities/ports for the Covered Region (similar to Crimea Sanctions Advisory) particularly for payment screening.
- Enhanced Due Diligence of all payment transactions associated with activities prohibited under SSI to confirm that licenses are in place.
- De-risking

Sanctions Risk for Crypto Activity

Even if Banks are not providing banking services to crypto entities, they may have indirect crypto sanctions exposure if their customers do transact in crypto from their US\$ accounts.

Risk	Risk Rationale	Action Plan
Underestimated crypto risk	Your customers may still send or receive funds tied to crypto transactions, even if your organization is not directly exposed to crypto risk through established relationships with crypto-based businesses.	Update OFAC risk assessment to include relevant crypto metrics such as: <ul style="list-style-type: none">- Population of customers engaging in crypto- Transactional volumes.
Incomplete customer risk profiles	Without a robust focus on crypto in KYC (CDD, EDD) and CRR controls, a financial organization may be unaware of the amount of crypto exposure it has within its customer base.	Update KYC and CRR controls to identify customers conducting crypto transactions including: <ul style="list-style-type: none">- Businesses accepting crypto payments- Customers who buy/sell crypto
Incomplete scenarios for crypto usage	Transaction monitoring systems not including crypto scenarios are unable to accurately identify crypto risk.	Update transaction monitoring systems to identify crypto transactions, including: <ul style="list-style-type: none">- Volume limits- Counterparty identification- IP screening
Ineffective sanctions screening, detection, and compliance	OFAC interdiction software is effective in identifying Sanctioned individuals and entities but may be not be as effective at identifying the original sender or ultimate beneficiary of a cryptocurrency transaction. Software	Update OFAC screening applications to identify payment transactions needing enhanced due diligence prior to processing, including risk-based: <ul style="list-style-type: none">- Internal list of crypto entities- Internal lists of cities in relevant territories

FinCEN's Red Flags for Sanctions Evasion Risk

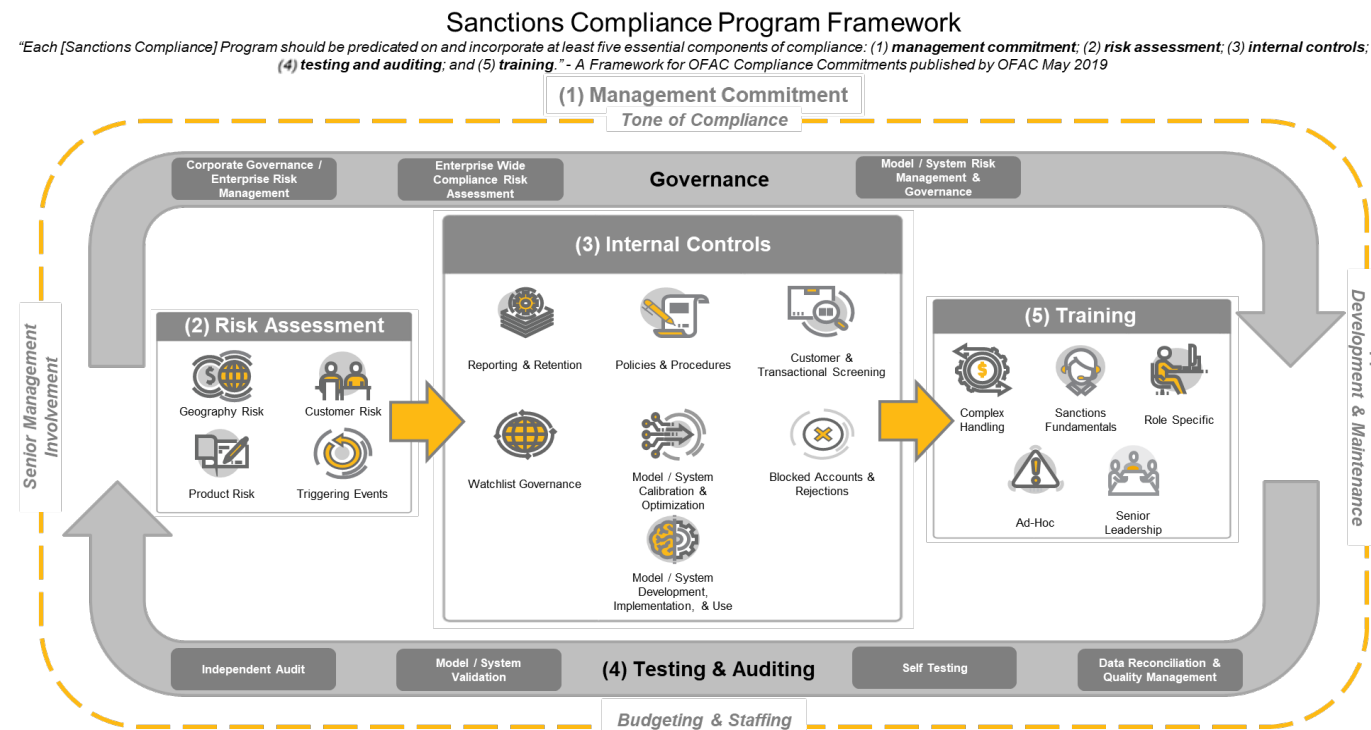
On 3/7/22, FinCEN issued Increased Vigilance for Potential Russian Sanctions Evasion Attempts, very comprehensive advisory related to sanctions risk

Red Flags

- Use of corporate vehicles to obscure connection (ownership, source of funds, etc.) to sanctioned jurisdictions sanctioned via Sectoral Sanctions (SSI)
- Use of shell companies
- Use of third parties to shield identity of sanctioned individuals
- New accounts/companies attempting to send/receive funds to/from institutions removed from SWIFT
- Non-routine Foreign Exchange (FX) transactions inconsistent with prior activity
- Transactions initiated from IP addresses associated with sanctioned jurisdictions
- Transactions connected crypto addresses associated with sanctioned individuals/entities (SDNs)
- Customers buying/selling crypto currencies via crypto exchanges in high risk jurisdictions.
- Rapid trades of crypto currency across various crypto exchanges

Sanctions Programs


OFAC's "A Framework for OFAC Compliance Commitments" issued in 2019 has never been as important. The Ukraine crisis has prompted OFAC and its global counterpart to issue an unprecedented number of new sanctions. Most organizations programs are focused on list-based entries such as the Specially Designated Nationals and Blocked Persons List (SDN) programs and may struggle to implement relevant investigative and monitoring controls to manage the complexity of Sectoral Sanctions.



*The Sanctions Compliance Program Framework is the intellectual property of Crowe, LLP.



Crypto



Crypto Market – 2021 Milestones

- 2021 was a record year for the cryptocurrency market:
 - Crypto market surpassed \$3 trillion in value in November 2021.
 - Bitcoin hit \$1 trillion in market value in February 2021 for the first time, and its price hit a record high of over \$68K in November 2021.
- Increase in crypto traders:
 - Verified users of the crypto exchange Coinbase grew to 73 million by September 2021, from 32 million at the beginning of 2019.
 - 16% of Americans say they have invested in, traded in, or used a cryptocurrency.
- Non-fungible tokens (NFTs) surged in popularity:
 - NFTs sold for millions of dollars alongside fine art in major auction houses.
 - Christie's became the first major auction house to sell a fully digital, NFT-based piece of artwork in March 2021.
 - NFT market had over \$23 billion in trading volume in 2021.
- Broad range of country acceptance:
 - El Salvador adopted Bitcoin as legal tender in June 2021
 - China banned cryptocurrency in September 2021
- The first US futures-based Bitcoin ETF launched in October 2021, trading on the NYSE under “BITO”
- Growth of Decentralized Finance (DeFi):
 - DeFi's Total Value Locked (TVL) surged by 300% year-to-date as more retail and institutional investors acknowledged it as an investment opportunity.
- Federal Reserve Board examining potential for a U.S. central bank digital currency.



Crypto Regulatory Updates

- OCC's Approval of Crypto Custody
 - OCC allowed federally chartered banks to provide custody services for crypto assets in June 2020.
 - U.S. Bank launched cryptocurrency custody services in October 2021.
 - Bank of NY Mellon, State Street, and Northern Trust also revealed plans to support crypto custody in Q4 2021.
- OCC Charters for Crypto-Focused Entities
 - In January 2021, the OCC granted a national trust bank charter to Anchorage Trust Company, making it the first “digital asset bank” in the U.S.
 - Protego Trust Company and Paxos were granted conditional OCC charters soon after.
- October 2021 FATF Guidance
 - Clarified anti-money laundering requirements for virtual asset service providers (VASPs), including licensing requirements, CDD measures, travel rule compliance, transaction monitoring processes, and suspicious transaction reporting.
- Federal Infrastructure Legislation (November 2021)
 - President Joe Biden signed an infrastructure bill into law which includes tax reporting provisions that apply to digital assets like cryptocurrency and NFTs.
- Enforcement Actions
 - BitMex (August 2021): Fined \$100 Million by both FinCEN and Commodity Futures Trading Commission for failure to establish a BSA Program.
 - Coinbase (September 2021): New “Lend” product launch was cancelled by the SEC due to their product being considered a security by the SEC.



SAR Exemptions

OCC Issues Final Rule Addressing Authority for Exemptions to Suspicious Activity Report Requirements

- ✓ For any SAR regulation exemption request, the OCC will consider criteria specified in the final rule, including consistency with the purposes of the Bank Secrecy Act and safe and sound banking.
- ✓ establishes processes for the OCC to facilitate changes related to SAR regulations required by the Anti-Money Laundering Act of 2020.
- ✓ establishes processes for the OCC to grant relief to banks that develop innovative solutions intended to meet Bank Secrecy Act requirements more efficiently and effectively.
- ✓ does not, by itself, result in any exemptions from SAR requirements. The final rule only clarifies the OCC's legal authority to issue such exemptions in the future.
- ✓ When issuing any exemptions, the OCC expects to coordinate with FinCEN and the other federal banking agencies. For exemption requests from the OCC's SAR regulations that would also require an exemption from FinCEN's SAR regulation, a bank would need to seek an exemption from both the OCC and FinCEN.
- ✓ Rule is effective May 1, 2022

FFIEC Exam Manual Updates

Introduction - Customers (new)

The following sections on different customer types are intended to be a subset of a broader review of compliance with BSA/AML regulatory requirements, such as customer identification, customer due diligence (CDD), beneficial ownership of legal entity customers, and suspicious activity reporting. **However, there is no BSA/AML regulatory requirement or supervisory expectation for banks to have unique or additional customer identification requirements or CDD steps for any particular group or type of customer.** Consistent with a risk-based approach, the level and type of CDD should be commensurate with the risks presented by the customer relationship.

BUT:

“Banks must have appropriate risk-based procedures for conducting ongoing CDD to understand the nature and purpose of customer relationships, and to develop customer risk profiles. The information collected to create a customer risk profile should also assist banks in conducting ongoing monitoring to identify and report any suspicious activity.



FFIEC Exam Manual Updates

“Specific information that would help understand the nature and purpose of the NPO” *

- * *Also sub in “ATM Owners or Operators”; or “Politically Exposed Persons”.*
- Note change from NGO to Charities and Nonprofit Organizations (NPO)





Enforcement Actions

Bank Secrecy Act / Anti-Money Laundering

Examiner expectations and pressure continue to persist as evidenced through continuing consent orders and regulatory actions.

- Updates to FFIEC are intended to improve transparency in the exam process. Examiners are focused on a risk-based approach placing greater focus on the BSA risk assessment and the independent audit.
- Additional focus on the Bank's BSA Compliance Officer and role of the Board in ensuring the BSA Officer is fully supported with "appropriate authority, independence, and access to resources to administer an adequate BSA/AML Compliance program based on the Bank's ML/TF and other illicit financial activity risk profile."

An identified shortcoming of an AML program is the lack of a strong compliance culture within the Bank, particularly within management. A compliance culture can be defined as the norms and values that a financial institution adheres to that are embedded in the everyday work that the employees carry out.



Bank Secrecy Act / Anti-Money Laundering

Supervision Priorities for BSA/AML include:

- Customer due diligence and beneficial ownership
- Whether BSA/AML risk management systems match the complexity of the business models and products offered
- Evaluating technology solutions to perform or enhance BSA/AML oversight
- Adequacy of suspicious activity monitoring and reporting systems and processes
- Overlapping issues of money laundering, fraud, consumer protection and cyber vulnerabilities



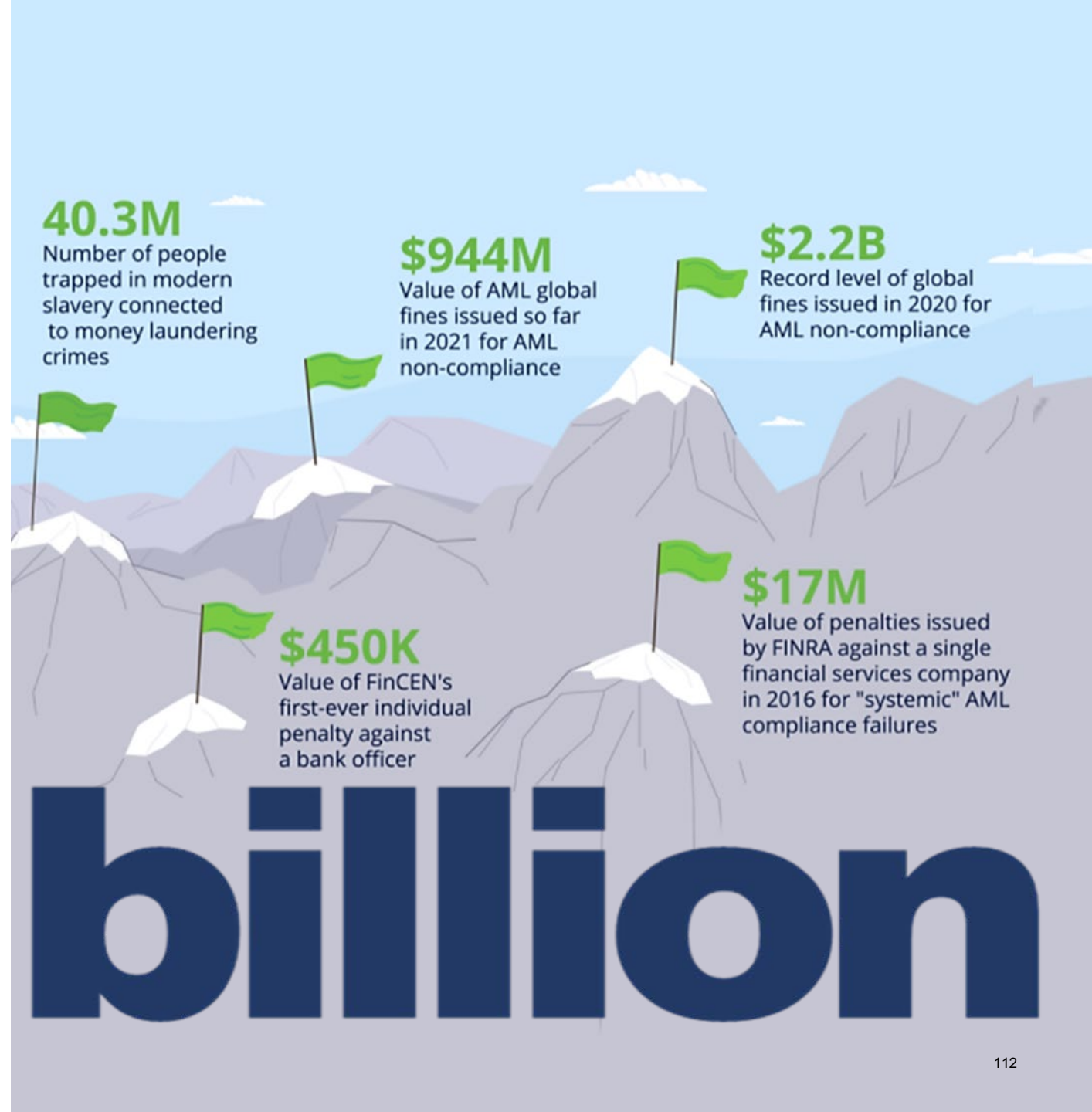
Enforcement Actions

AML fines globally is expected to hit over \$2 billion potentially surpassing the record set in 2020 of \$2.2 billion.

Not only are firms penalized for AML non-compliance. In March 2020, FinCEN issued a \$450,000 civil money penalty on an individual bank officer.

Increasing fines and penalties for sanctions violations.

\$2.2



Enforcement Actions



Recent examples of global enforcement actions due to failures within the institution's AML program:

- December 2021 – NatWest fined nearly 265 millions (pounds) for AML failures. The FCA indicated the UK-based financial institution was fined for failing to properly monitor the activity of a commercial customer between November 2012 – June 2016. The initial due diligence indicated limited cash and annual sales of 15 million. Over four (4) years 50 NatWest branches received cash from the jewelry dealing depositing as much as 1.8 million in cash each day. NatWest was fined for failing to flag and investigate this customer.
- December 2021 – FinCEN fined Community Bank of Texas \$8 million for violations of the BSA. The Bank's consent order stated the Bank was understaffed and inadequately resourced. The Bank also indicated they failed to report suspicious transactions for their customers to FinCEN from 2015 – 2019. Additionally, the OCC fined the Bank \$1 million.
- January 2021 – FinCEN fined Capital One \$390 million for BSA violations. Capital One admitted that from at least 2008 through 2014 it failed to file around 50,000 Currency Transaction Reports worth over \$16 billion, which were linked to organized crime, tax evasion, fraud, and other financial crimes.

Enforcement Actions

The purpose of BSA regulatory enforcement actions is meant to ensure compliance with the requirements of the BSA, the rise in BSA enforcement actions may cause both the financial industry and regulatory authorities to re-examine BSA regulation and enforcement and their effectiveness at fulfilling the purposes of the AML/CFT regime.

Recent actions demonstrate that despite the government's work to ease regulations, regulators continue to rigorously enforce BSA/AML compliance at financial institutions.

Financial institutions not meeting their obligations under the BSA or correcting known deficiencies can lead to greater scrutiny, significant fines, operational and reputational risks and potentially even a criminal conviction.



Enforcement Actions

Criminal Penalties for willful BSA regulations violations can cost you!

"A person convicted of money laundering can face up to 20 years in prison and a fine of up to \$500,000.

Any property involved in a transaction or traceable to the proceeds of the criminal activity, including property such as loan collateral, personal property, and, under certain conditions, entire bank accounts (even if some of the money in the account is legitimate), may be subject to forfeiture.

... the U.S. Department of Justice may bring criminal actions for money laundering that may include criminal fines, imprisonment, and forfeiture actions. In addition, banks risk losing their charters, and bank employees risk being removed and barred from banking."



Enforcement Actions



Three **(3)** trends can be found in BSA enforcement:

- 1) an increase in the frequency and size of penalties;
- 2) an emphasis on the acceptance of responsibility by institutions; and
- 3) the increased risk of individual liability.

Remember FinCEN's \$1 million civil money penalty against Thomas Haider?

Haider was the former chief compliance officer of MoneyGram International. FinCEN found Haider guilty of willful violations of BSA program requirements and not filing suspicious activity reports.

FinCEN's enforcement action was brought before the courts over the application of the BSA to individuals. The court found in favor of FinCEN and that Haider could be held liable for violations of the BSA's AML program requirements.

The case was settled in 2017 with Haider agreeing to pay a \$250,000 fine and be barred from a similar job for three (3) years.



BSA/AML– What’s Next?

- **Continued emphasis on BSA/AML Investigations:** federal, and state regulators/examiners remain focused on BSA/AML compliance. Regulators and examiners maintain focus on financial institutions’ response to COVID-19.
- **Broad Application of AML Requirements:** Actions against crypto-businesses illustrate the broad view U.S. regulators are taking in mandating adequate AML compliance. Developments in application of BSA rules to sports betting, additional crypto regulations, further attention on the real estate industry, and enactment of pending legislation may bring about further change.
- **FinTech:** Legislators and regulators will continue to try to ensure that financial technology platforms are not used for money laundering.
- **Corporate Governance:** Sanctions and AML regulators are increasingly interested in corporate compliance.
 - Compliance requirements in recent OFAC settlements.



Focus on the effectiveness of your program overall.



Thank you!



John Bono
CAMS
919.521.7210
john.bono@crowe.com

"Crowe" is the brand name under which the member firms of Crowe Global operate and provide professional services, and those firms together form the Crowe Global network of independent audit, tax, and consulting firms. Crowe may be used to refer to individual firms, to several such firms, or to all firms within the Crowe Global network. The Crowe Horwath Global Risk Consulting entities, Crowe Healthcare Risk Consulting LLC, and our affiliate in Grand Cayman are subsidiaries of Crowe LLP. Crowe LLP is an Indiana limited liability partnership and the U.S member firm of Crowe Global. Services to clients are provided by the individual member firms of Crowe Global, but Crowe Global itself is a Swiss entity that does not provide services to clients. Each member firm is a separate legal entity responsible only for its own acts and omissions and not those of any other Crowe Global network firm or other party. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global. The information in this document is not – and is not intended to be – audit, tax, accounting, advisory, risk, performance, consulting, business, financial, investment, legal, or other professional advice. Some firm services may not be available to attest clients. The information is general in nature, based on existing authorities, and is subject to change. The information is not a substitute for professional advice or services, and you should consult a qualified professional adviser before taking any action based on the information. Crowe is not responsible for any loss incurred by any person who relies on the information discussed in this document. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global. © 2022 Crowe LLP.

Appendix

Strengthening Treasury Financial Intelligence AML, and CFT Programs



This section focuses primarily on changes within U.S. government structures and its relationship to foreign Financial Intelligence Units (“FIU”). There is emphasis on the importance of the U.S. government working closely with foreign counterparts in the sharing of information.

Key Points to Remember:


- Establishes national examination and supervisory priorities

- FinCEN now required to facilitate a voluntary public-private information sharing partnership among law enforcement agencies, national security agencies, financial institutions and FinCEN.

- Expands AML/BSA requirements to antiquities dealers.

- Amends Section 5312(a)(2) of Title 31, USC to expand definition of “funds” to include digital currencies.

Modernizing the AML and CFT System



This section of the 2021 NDAA will have a direct impact on organizations' FIU operations, as it emphasizes the usage of data and technology. One of the significant changes recommended within the 2021 NDAA is the evaluation of the reporting thresholds. As systems are tuned and configured to identify activity that occurs within thresholds, additional tuning exercises may be required.

Thresholds for structuring rules are directly related to the current \$10,000 reporting threshold. If the threshold was raised, a financial institution's model configuration would need to be adjusted or alerts would be generating without adding value to the monitoring program.

Key Points to Remember:

- Streamlined opportunities and potential new thresholds for CTRs and SARs.
- Creation of new standard for how financial institutions test their technology.
- Creation of pilot program for FIs to share SAR info with their foreign branches, subsidiaries and affiliates.
- Permission for two or more financial institutions to collaborate and share compliance resources.
- FinCEN required to report semi-annually on threat patterns and trend data.

Improving AML and CFT Communication, Oversight and Processes




This section focuses on promoting cooperation with law enforcement by incentivizing individuals to come forward and report illicit activity, while also creating harsher penalties for those who do not comply with BSA/AML law. Whistleblowers are specifically mentioned and now receive increased protections and a newly established private right of action if the whistleblower suffers retaliation for disclosing BSA violations.

Key Points to Remember:

- Additional safe harbors for financial institutions cooperating with law enforcement Keep-Open letters.
- Provides DOJ increased ability to subpoena the records of foreign banks that maintain correspondent accounts in U.S.
- Significant increases to damages/penalties for BSA/AML non-compliance.
- Increased protections and potential rewards for whistle-blowers to incentivize the reporting of BSA/AML violations.

Establishing BO Information Reporting Requirements



The 2021 NDAA **requires** FinCEN to maintain a secure, non-public database as a registry of Beneficial Owner (“BO”) information collected for companies that are based in or operating within the U.S. LLCs, corporations, and other similar entities will now have to provide ownership information to FinCEN. Under the Act, ownership is defined as:

“An individual who, directly or indirectly, through any contract, arrangement, understanding, relationship, or otherwise (i) exercises substantial control over the entity; or (ii) owns or controls not less than 25 percent of the ownership interest of the entity.”

Key Points to Remember:

- FinCEN will be required to maintain a registry of beneficial ownership information in a secure, non-public database collected for certain U.S. companies and companies doing business in the U.S.
- FIs will be able to request information from the FinCEN Beneficial Ownership database with consent from the reporting company if subject to the CDD requirements.
- FinCEN will be required to eventually revise the CDD Final Rule to reduce burdens on FIs and legal entity customers that are unnecessary or duplicative.
- Requirements established for law enforcement and other government agencies to access the FinCEN database.

Miscellaneous



The AML/BSA reform included in the 2021 NDAA concludes with a “Miscellaneous” section. This section includes the expansion of SEC enforcement power, creating a 10-year statute of limitations for the SEC to seek disgorgement. The Act also places processes for the Government Accountability Office (GAO) and Department of the Treasury to evaluate trends related to financial crimes risk.

The regulatory landscape continues to evolve and FinCEN will be communicating additional action items for organizations to implement to adhere to the newly enacted regulations in the future.

Key Points to Remember:

- Amends the Securities Exchange Act of 1934, expanding SEC enforcement power to seek disgorgement.
- Includes provisions for numerous studies to be performed by the GAO and the Department of the Treasury.

FinCEN Achievements to Date



- February 24, 2021 – Announcement of the Financial Crimes Tech Symposium
- February 26, 2021 – Direct Hire Authority Operationalized
- March 9, 2021 – FinCEN Notice on Trade in Antiquities and Art
- March 23, 2021 – First FinCEN Exchange Since Codification of Program
- March 26, 2021 – Innovation and Emerging Technologies Briefing to the Senate Committee on Banking, Housing, and Urban Affairs and the House Financial Services Committee and Publication of Supporting Report on FinCEN's Innovation Hours Program
- April 1, 2021 – Beneficial Ownership Advance Notice of Proposed Rulemaking
- May 19, 2021 – Bank Secrecy Act Advisory Group Plenary Session, Announcing the Launch of New Subcommittees on Innovation and Technology and Information Security and Confidentiality
- June 28, 2021 – No-Action Letter Assessment Submitted to Congress
- June 30, 2021 – Publication of National AML/CFT Priorities and Related Guidance
- September 23, 2021 – Advanced Notice of Proposed Rulemaking for Arts and Antiquities
- October 15, 2021 – Ransomware Trends in BSA Data from January to June 2021
- December 7, 2021 – Notice of Proposed Rulemaking to implement Beneficial Ownership information reporting provisions of CTA
- December 14, 2021 – Request for Information for Review of Regulations and Guidance
- December 20, 2021 – Illicit Finance Threat Involving Wildlife Trafficking and Related Trends in BSA Data
- January 24, 2022 – SAR Sharing Pilot Program