

How Activision Blizzard streamlined repetitive tasks and improved productivity in Internal Audit

Artur Cieplik
Senior Director, Internal Audit

Geoffrey Dollin
IT Audit Supervisor

January 26, 2022



Housekeeping

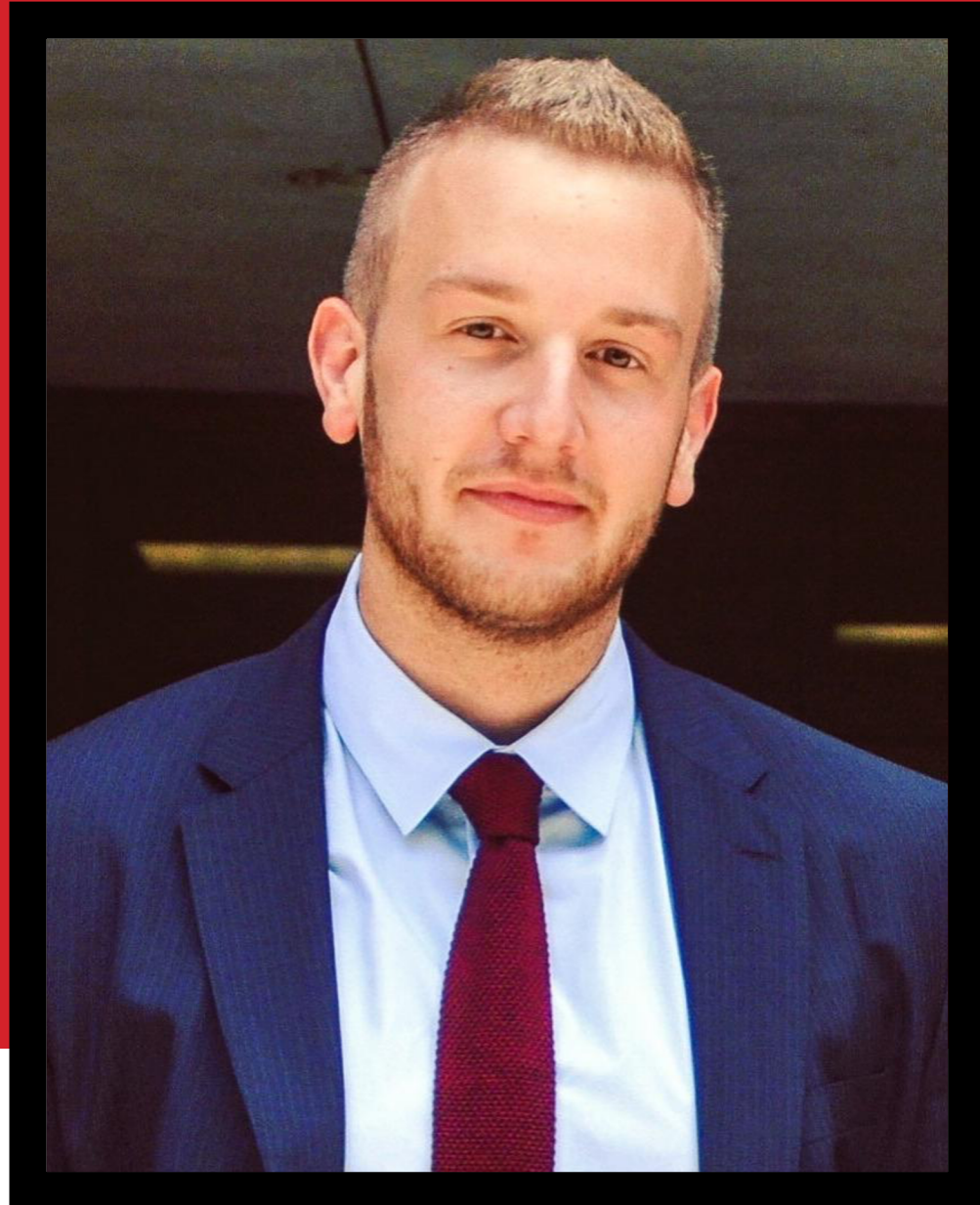
- Today's session will be 45 minutes with 15 minutes for Q&A.
- Please submit your questions through the Q&A panel on your GoToWebinar console.
- This session will be recorded. We will send a copy of the recording and slides to all attendees.



Artur Cieplik

- *Senior Director*

Artur leads the Global IT Audit and Data Analytics team delivering high-caliber audits and IT SOX compliance. Artur's career spans over 14 years with IT Audit roles at British Airways, BMW, Tesco and King.



Geoffrey Dollin

- *IT Audit Supervisor*

Geoffrey is an experienced IT audit, data analytics and automation professional. His time is split between IT audit and spearheading the internal audit group's data analytics and automation efforts. Before joining Activision Blizzard, he worked at RSM US LLP in technology risk consulting.

Agenda

- Introduction
- Overview and Structure of Internal Audit at Activision Blizzard
- Before Diligent
 - Data Analytics
 - SOX Testing
 - Continuous Monitoring
- Solution
- Results

Overview of Activision Blizzard

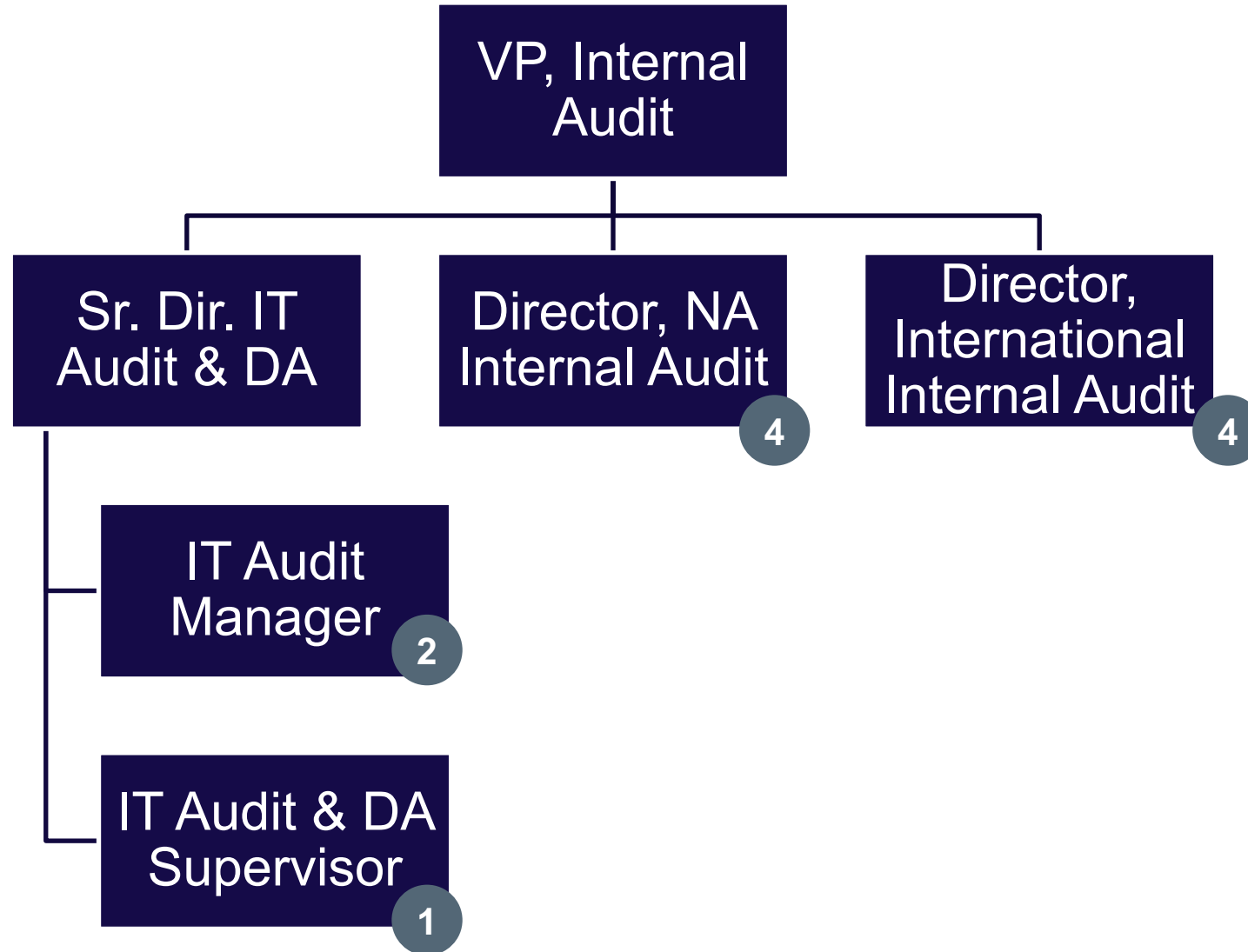


Activision Blizzard makes and publishes video games on console, PC, and mobile. Activision Blizzard continues to be one of the most influential and successful interactive entertainment companies in the world.

How Internal Audit Operates at Activision Blizzard

- Internal Audit is a global function that operates across all business units
 - Focus on delivering on a mission of providing independent assurance and business process advisory
 - Responsible for delivering an operational audit plan and SOX testing
- IT Audit and Data Analytics team focuses on IT operational audits, IT SOX, Data Analytics and Automation

Organizational Chart of Internal Audit



Poll Question #1

How would you rate your organization's internal audit data analytics capability?

- A. We don't use data analytics in internal audit
 - B. We only barely use data analytics
 - C. We have an average data analytics capability
 - D. We have a robust data analytics capability
-

The Before Scenario

Before Diligent

- Very limited data analytics capabilities in the team, external partners used for data analytics during operational audits
- No automation for manually performed SOX controls testing
- No effective continuous monitoring solutions

Before Diligent

Data Analytics – Operational Audits

- Time spent manually obtaining, manipulating and normalizing data provided by stakeholders
- Difficulty handling large volumes of data within Excel
- Limited coverage using sample-based testing and standard sampling methodologies: random, haphazard, judgmental, etc.
- Possibility for human error in manual data interpretation, sampling, and testing

Before Diligent

SOX Testing

- Internal Audit team spent a great deal of time meeting with stakeholders, requesting data, gaining comfort over data generation, and documenting
- Through these efforts, and through multiple phases of SOX testing each year
 - time was spent following up on requests for evidence and documenting completeness and accuracy
 - audit fatigue was setting in with some of the business stakeholders
 - there was an increased likelihood of human error in testing

Before Diligent

Continuous Monitoring - Vendor Banking Changes

- Following an increase in business email compromise attempts, Activision began to begin work to introduce automation to detect and predict fraud
- Business and finance controls had little automation and providing coverage for these risks was highly manual
- Due to manual processes, Activision was potentially vulnerable to evolving threats from sophisticated bad actors

Poll Question #2

How advanced is your use of continuous monitoring in internal audit?

- A. We don't use continuous monitoring in internal audit
 - B. We only barely use continuous monitoring
 - C. We have an average continuous monitoring capability
 - D. We have a robust continuous monitoring capability
-

Looking for a solution

Three Pillars

Solution

ACL Robotics

- ACL Robotics is a Diligent product that contains Analytics, Robots, Results, and Storyboards. ACL Robotics optimizes the way governance professionals work by automating time-intensive and repetitive – but critical – business processes.
 - Automate scripts
 - ACL Robotics provides an easy way to take Analytics scripts that you currently run ad hoc in Analytics, and run them on an automated schedule in the Robots app.
 - Free up time and resources
 - Using ACL Robotics, you can automate repetitive tasks and free up time and resources for you and your team to perform work of a more strategic nature.
 - View results
 - You can export the output results of the automated scripts to the Results app for processing, issue remediation, and data visualization. You also have the option of opening the output results in Analytics.

Solution

3 pillar automation and data analytics strategy

Data Analytics in Operational Audits

- Leverage ACL Robotics to increase audit coverage and accuracy

SOX Controls Testing Automation

- Automate testing data collection, sample selections and manual testing procedures

Continuous Monitoring Solutions

- Implement solutions to mitigate key business process and IT risks

Solution

Required capabilities

- System connections to applications and tools
 - SOX in-scope systems
 - Read only access
- Practical SQL scripting knowledge
 - Used to access data and create data pulls
- ACL and Python scripting knowledge
 - Used for automation and data manipulation

Solution

Key success factors

- Leveraged Diligent training library for skilling up the IA team
- Held brainstorming sessions to identify viable use cases leveraging the in-depth business process knowledge within the IA team
- Developed an automation roadmap and assigned projects to volunteers within the team
- Established lightweight internal standard operating procedures for Diligent projects
- Engaged with external auditors to clear Diligent's use for SOX testing automation

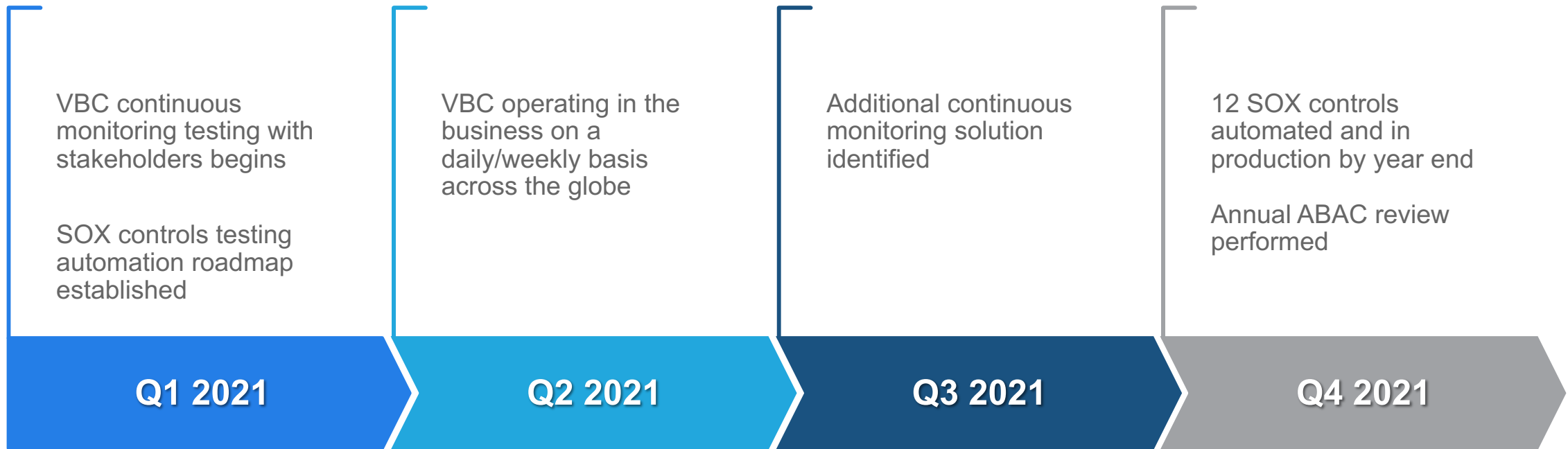
Solution

Timeline



Solution

Timeline



Solution – Data Analytics

Anti-bribery and Anti-corruption (ABAC) Audit

- Use ACL to identify high risk transactions based on, but not limited to;
 - keyword searches
 - outlier transactions
 - one-time payments to vendors
 - even amount transactions
 - vendors with above average payment amounts and below average frequency of payments
- Use ACL to analyze 100 percent of transactions
- Increased analytic accuracy, removing the possibility of human error

Solution – Data Analytics

ABAC test script examples

Test Name	Description / Logic	Risk Score	Data Used
Keywords	Keyword searching for gifts & donations on journal entries	+1 for each keyword hit. If the same keyword is hit multiple times, there is still just +1 added to the risk score but if multiple keywords are hit, there will be +1 for each unique keyword hit.	Journal Entries; The fields searched were: JE_Line_Description, JE_Header_Description, JE_Batch_Description
Outlier Journal Entry Transactions	This test selects journal entries that deviate more than 2 standard deviations from the average posted amount to the account	+1 for each journal entry that has an accounted_net_amount that is outside of 2 standard deviations of the average for the GL account	Journal Entries; The averages and deviations are calculated on the field “Accounted_Net_Amount_USD”
High Amounts Low Frequencies	This tests flags those vendors with an above average payment amount but a below average frequency of payments	+1 for each vendor that has an above average amount and a below average frequency	P2P transactions; The CHECK_AMOUNT field is used to calculate the total payment amount to each vendor
Even Amounts	This analytic looks for journal entries that are from the T&E accounts, then calculates if the amount in the “Accounted_Net_Amount” field ends in an even amount	+1 for each journal entry with an even amount in the Accounted_Net_Amount field	Journal Entries; The field “Accounted_Net_Amount” is used to look for even amounts

Solution – SOX Testing

Automate SOX testing

- Throughout 2021, Internal Audit has leveraged ACL robotics to automate 12 SOX controls
 - Automations vary from population and sample generation to complete control testing and documentation
 - Example controls automated:
 - Business Process control – JE Approval SOD
 - Business Process controls – PO and Invoice approvals
 - IT controls – Terminations (100 percent testing)
 - IT controls – Passwords (automated data and requirements comparison)

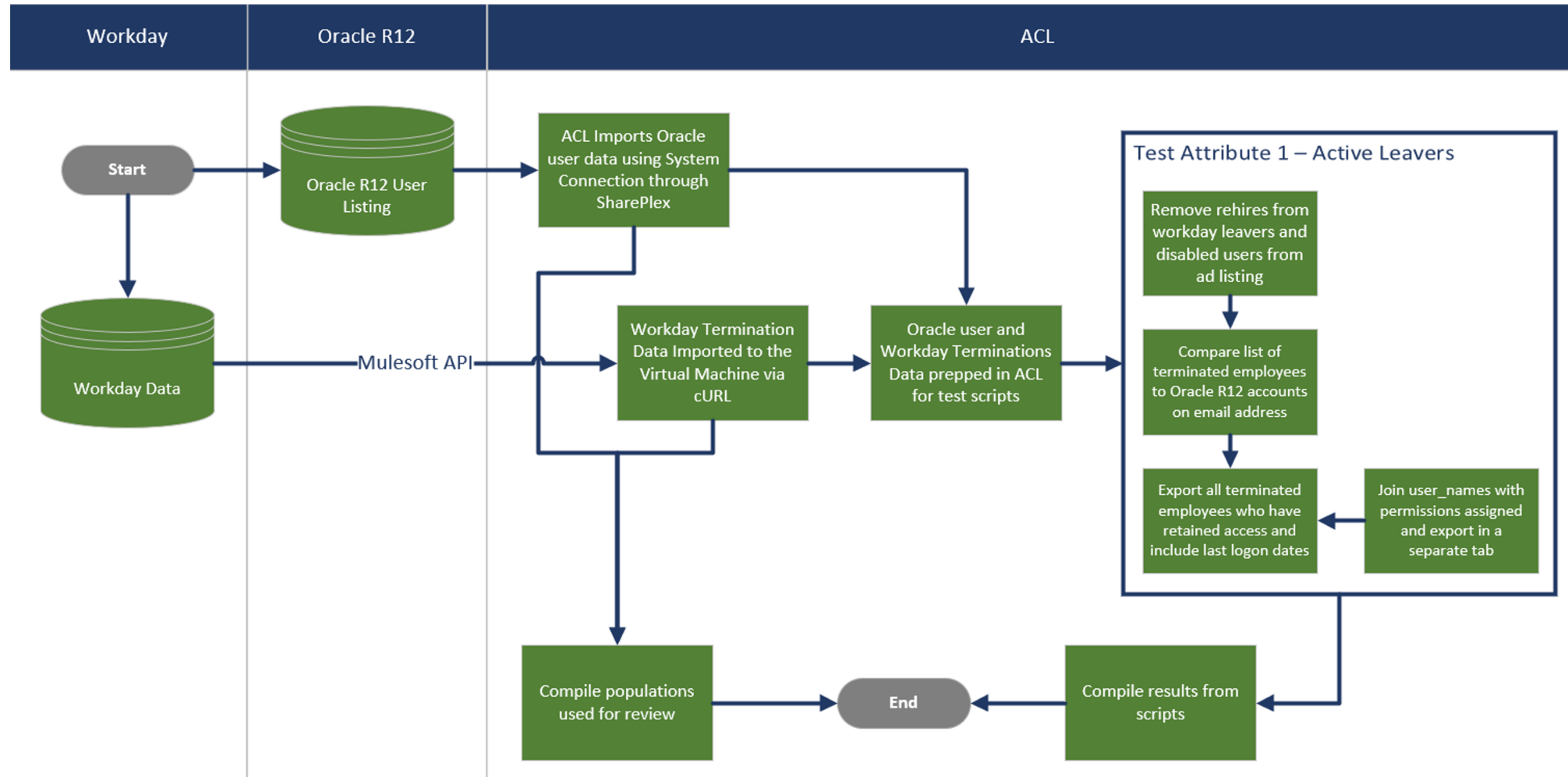
Solution – SOX Testing

Things to consider when getting started

- Target controls with a low degree of complexity and high return on investment
 - I.e., terminations testing is relatively simple but takes a lot of time to manually document and complete across all the applications and multiple times throughout the year
- Partner with your external auditors or regulators to ensure they are comfortable relying on the work and the change management processes

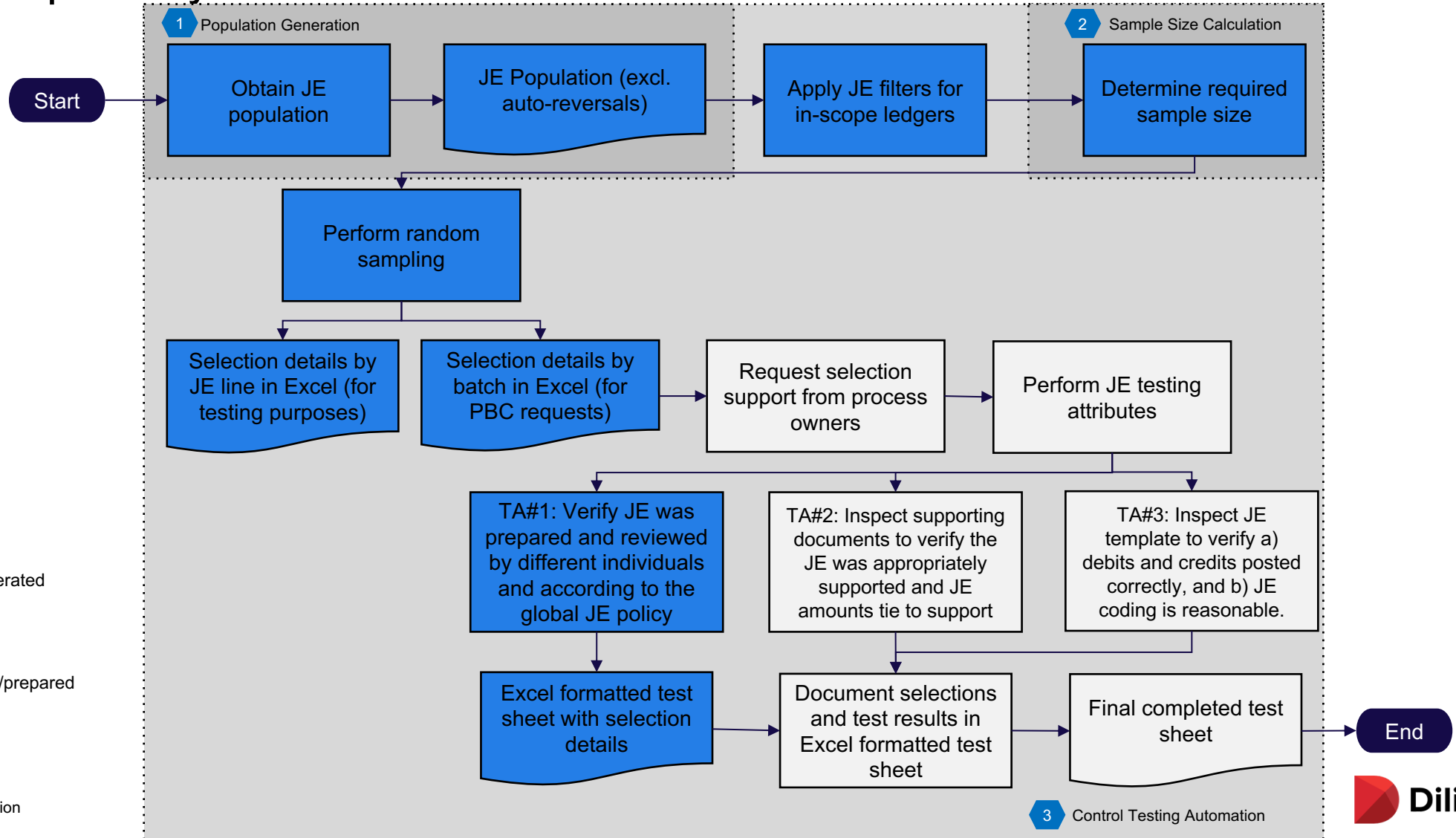
Solution – SOX Testing

IT Control – fully automated



Solution – SOX Testing

BP Control – partially automated

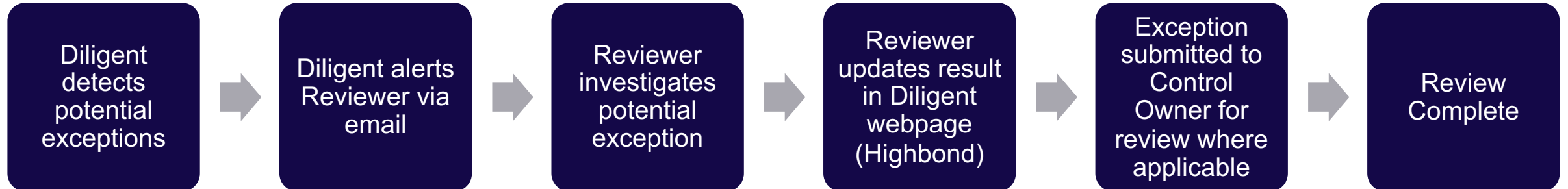


Solution – Continuous Monitoring

Vendor Banking Changes: automate testing and remediation workflows

This automated solution to the vendor banking change control monitoring has three basic steps:

1. Detection of potential exceptions
2. Notify regional P2P teams of potential exceptions
3. Provide a website to record investigation results of the potential exceptions



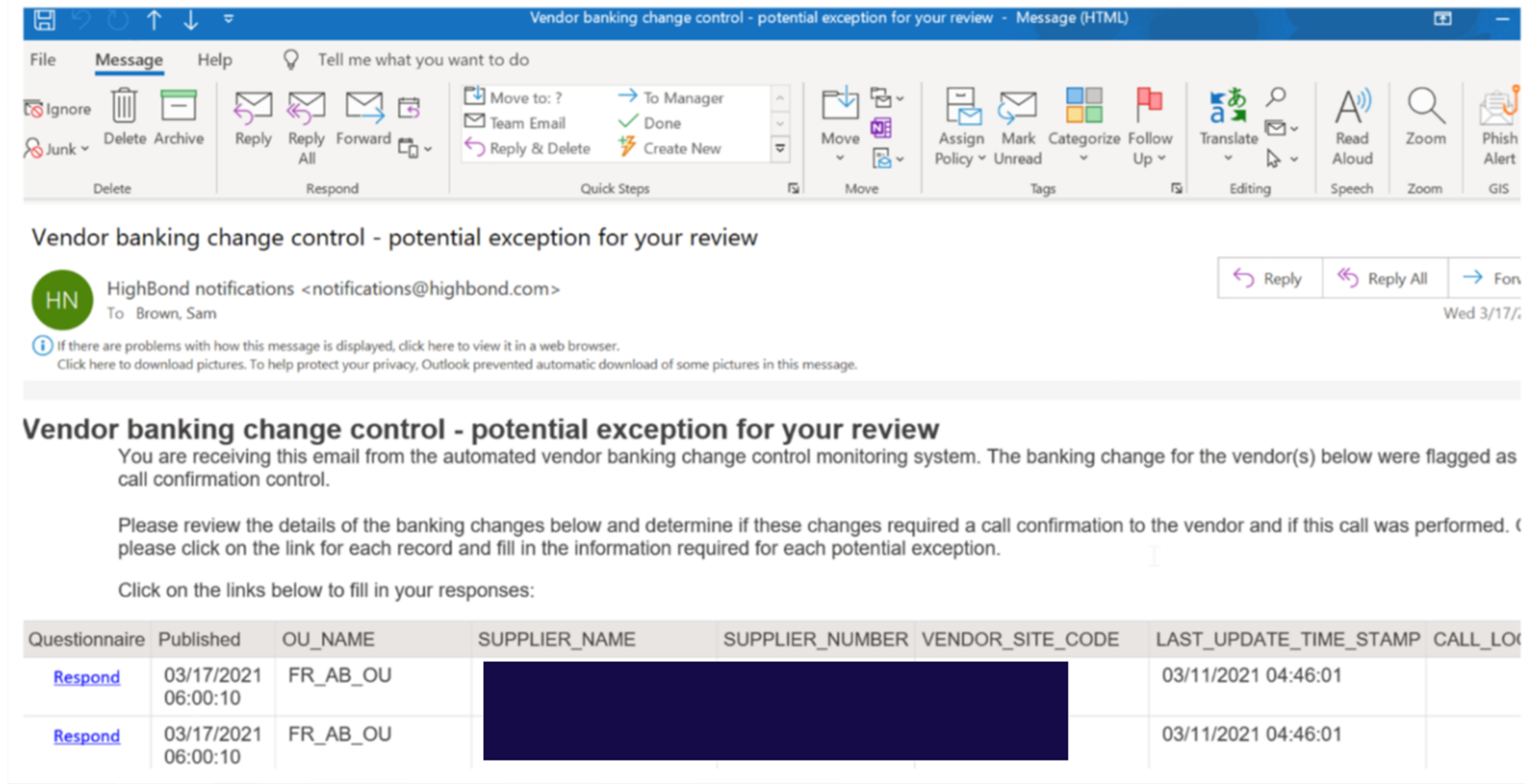
Solution – Continuous Monitoring

Vendor Banking Changes (VBC): automate testing and remediation workflows

- In March 2021, Internal Audit implemented ACL Robotics into VBC and launched global beta testing, detecting exceptions
- Through beta testing, process improvements were identified in the automation and implemented for the production version
- Now, the automation is self driving, runs daily/weekly across the entire organization

Solution – Continuous Monitoring

Vendor Banking Changes: example email notification



The screenshot shows an Outlook email window titled "Vendor banking change control - potential exception for your review - Message (HTML)". The email is from "HighBond notifications <notifications@highbond.com>" to "Brown, Sam". The subject is "Vendor banking change control - potential exception for your review". The body of the email contains the following text:

Vendor banking change control - potential exception for your review

You are receiving this email from the automated vendor banking change control monitoring system. The banking change for the vendor(s) below were flagged as call confirmation control.

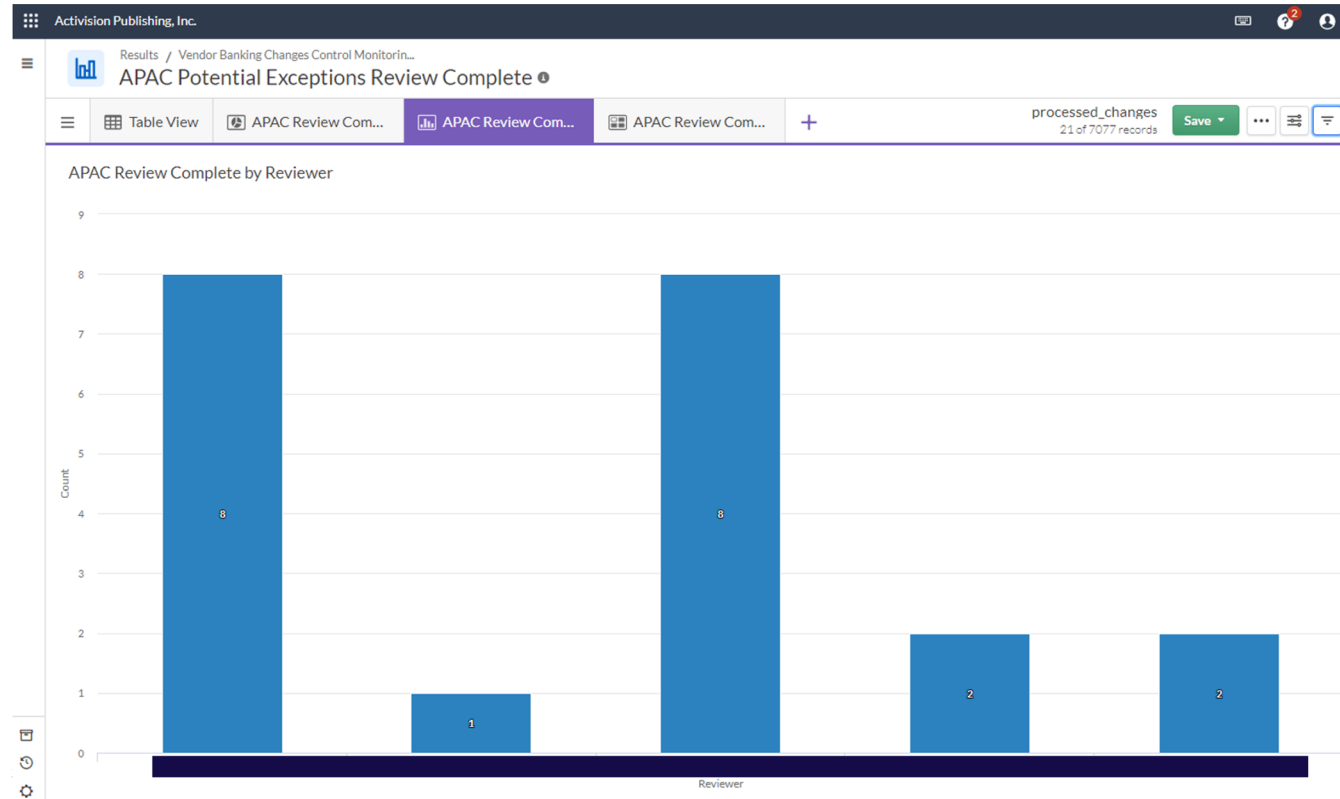
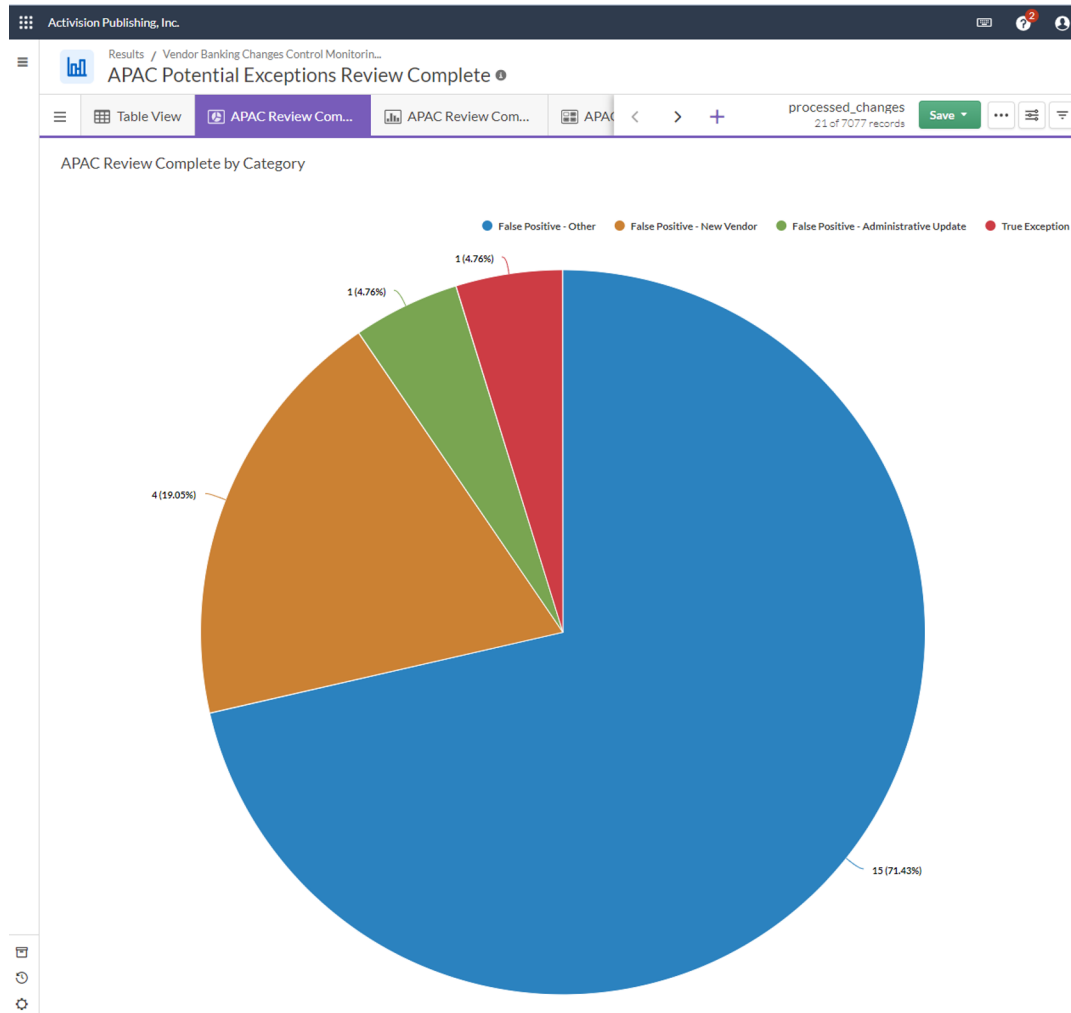
Please review the details of the banking changes below and determine if these changes required a call confirmation to the vendor and if this call was performed. (please click on the link for each record and fill in the information required for each potential exception.

Click on the links below to fill in your responses:

Questionnaire	Published	OU_NAME	SUPPLIER_NAME	SUPPLIER_NUMBER	VENDOR_SITE_CODE	LAST_UPDATE_TIME_STAMP	CALL_LO
Respond	03/17/2021 06:00:10	FR_AB_OU	[REDACTED]			03/11/2021 04:46:01	
Respond	03/17/2021 06:00:10	FR_AB_OU	[REDACTED]			03/11/2021 04:46:01	

Solution – Continuous Monitoring

Vendor Banking Changes: dashboards and storyboards



Solution – Continuous Monitoring

In Development

Develop and implement an automated solution for terminations monitoring that alerts key IT stakeholders of the following scenarios:

1. Terminated individuals who have retained access to Active Directory and/or key systems
2. Accounts whose access was removed after their termination date

The After Scenario

Results and usage

Positive Business Outcomes

Three Pillars			
	Data Analytics for IA operational audits and projects	SOX controls testing automation	Implementation of continuous monitoring solutions
Benefits	<ul style="list-style-type: none">• Time savings for Internal Audit team preparing and analyzing large data sets manually• Analyzed 100% of transactions, providing substantially increased assurance• Reduced risk of manual sampling/human errors• Improved testing accuracy	<ul style="list-style-type: none">• <u>Internal Audit time savings</u> (~10 hours per control) and efficiency gains – freeing up staff time to work on non-SOX projects. Total annual time savings ~120 hours.• <u>Stakeholder time savings</u> (~3 hours per control) and efficiency gains from the business stakeholders not having to manually provide documentation. Total annual time savings ~36 hours.• Improved testing accuracy	<ul style="list-style-type: none">• Mitigated fraud risks and increased assurance associated with changes to vendor banking details• Time savings across the business units, regional teams and Internal Audit• Scheduled automated checks to determine if system access removals were missed• Identification of pain points and/or delays in access removal processes across the organization

Measures of success

Across our three pillars

- Increased audit coverage
- Improved risk posture
- Time savings throughout internal audit and the stakeholders
- Improved testing accuracy
- Mitigated fraud risks

Key takeaways

- Identify practical use cases that offer a good return on investment
- Collaborate and engage with the broader internal audit team
- Leverage the scripts stored in Diligent's Script Hub
- Leverage relationships with the business/stakeholders/IT to establish broad system connections
- Partner with your external auditors and/or regulators

Poll Question #3

Are you interested in investing in a GRC solution in the next 6 months?

A. Yes

B. No

C. I don't know

Questions & Answers
