ACUA Webinar

The New Era of Fraud in Higher Education

02/27/2025

Virtual Learning Committee

Director
Wendee Shinsato, CPA, CIA
Assistant Vice Chancellor
California State University

Volunteer
Christiana Oppong, CIA, CCSA
Senior Auditor
Princeton University

Volunteer
Brenda Auner, CIA, CFE
Senior Auditor
California State University

Volunteer
Virginia L. Kalil, CIA, CISA, CFE, CRISC
Chief Internal Auditor
University of South Florida

Diligent

The New Era of Fraud in Higher Education

Integrating audit & ERM to navigate and mitigate unique risks for colleges & universities

Katja Freeman, Solution Sales Director – Public Sector

Chris Trepte, Solution Sales Director – Public Sector

February 27, 2025

The New Era of Fraud in Higher Education

Fraud in higher education presents significant financial, reputational, and operational risks. Participants will gain a deeper understanding of fraud risks unique to colleges and universities such as student aid fraud, financial fraud, and cybersecurity threats, and options to mitigate those risks.

Today we will:

Discuss how internal audit and an ERM program can work together to proactively detect, prevent, and respond to fraud in higher education, and understand strategies for integrating fraud risk management into audit planning, leveraging data analytics for fraud detection, and aligning and collaborating with enterprise risk management programs.

Learning Outcomes:

1. Identify unique fraud risks in higher education
2. Evaluate and align how audit and an ERM program can collaborate for a risk-based approach
3. Understand technology options for continuous monitoring and continuous risk assessments

Diligent

Bio

Katja Freeman, Solutions Sales Director, Audit, Risk & Compliance

- Since 2022, Katja has worked as a domain expert for Public Sector, Audit, Risk & Compliance at Diligent (formerly Galvanize and ACL). She previously spent 10 years at the City and County of Denver's Auditor's Office, rising from Senior Auditor to Audit Director, and nearly three years as a Performance Evaluator for Wyoming's Legislative Service Office.

- Katja holds master's degrees in Political Science and Environmental Policy, along with an audit analytics certificate from Rutgers University. She has led performance, IT, financial, and audit analytics teams, earning multiple awards from the Association of Local Government Auditors (ALGA). She also chaired ALGA's Professional Issues Committee on auditing standards.

Diligent

Bio

Chris Trepte, Solutions Sales Director

- With an IT background, Chris has held consulting roles managing client engagements focused on IT General Controls, SOC 2 Readiness, ICFR, SOX, NIST Compliance, and IT Security reviews.

- In March 2022, he transitioned to Diligent, first as a Client Partner in Customer Success, then managing implementations in Professional Services, and now as a Solutions Sales Director. Across these roles, he has driven client success, GRC technology adoption, and growth.
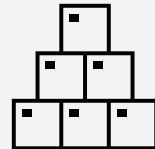

Diligent

Learning Objectives

1. Identify unique fraud risks in higher education

2. Evaluate and align how audit and an ERM program can collaborate for a risk-based approach

3. Understand technology options for continuous monitoring and continuous risk assessments

Diligent

Agenda

1. Introductions

2. Fraud vs. improper payments

3. How can auditors and risk managers collaborate in alignment with standards?

4. Unique fraud risks in Higher Education

5. Example: Vendor fraud

6. Continuous risk assessment and internal controls monitoring

7. How can technology tools help?

8. Analytics , automation, visualization

What is Fraud?
How is it different from improper payments?

Diligent

Fraud Triangle

Opportunity

- *Decentralized environment*
- *Sensitive information*
- *Different funding streams*

- *More people are financially impacted*

Incentive

Rationalization

Fraud Triangle

Opportunity

- *Decentralized environment*
- *Sensitive information*
- *Different funding streams*
- *Remote work*
- *Reliance on technology*
- *More vendors*

- *More people are financially impacted*

- *People don't appreciate me*
- *Everything is so expensive now*

Incentive

Rationalization

Polling Question #1

Does your institution conduct regular fraud training for all employees?

a. Yes
b. No
c. I don't know

"The typical amount of revenue lost to fraud is reported at 5%" (in reference to occupational fraud)

ACFE 2024, Report to the Nations

->This number has not changed from previous years.

Diligent

Improper Payments

What is it?

Definition: Funds that are disbursed which are either incorrect in amount or made to the wrong recipient

Examples:

- Federal student aid misallocation

- Funds disbursed to ineligible individuals, overpayments, underpayments

- Misuse of institutional funds: unauthorized expenses, use of P-Card instead of master purchase agreement, unauthorized use of T&E card

Occupational Fraud
ACFE Report to the Nations 2024

What do we learn from this graph?

- Web-submitted or emailed tips (rather than telephone) are most effective

- Data shows need for stronger use of preventive controls

Source: ACFE, Report to the Nations 2024, p. 24.

FIG. 13 HOW IS OCCUPATIONAL FRAUD INITIALLY DETECTED?

Tip	43%
Internal audit	14%
Management review	13%
Document examination	6%
Account reconciliation	5%
By accident	5%
External audit	3%
Automated transaction/data monitoring	3%
Surveillance/monitoring	2%
Other	2%
Notification by law enforcement	2%
Confession	1%

FIG. 14 WHO REPORTS OCCUPATIONAL FRAUD?

Employee	52%
Customer	21%
Anonymous	15%
Vendor	11%
Other	7%
Shareholder/owner	1%
Competitor	1%

Diligent

Organization-Wide Effort

- **Prevention**
- **Detection**
- **Improvements**

Compliance Management

Information Security

Third-Party Risk

Fraud Detection & Monitoring

Audits and Investigations

Risk Management
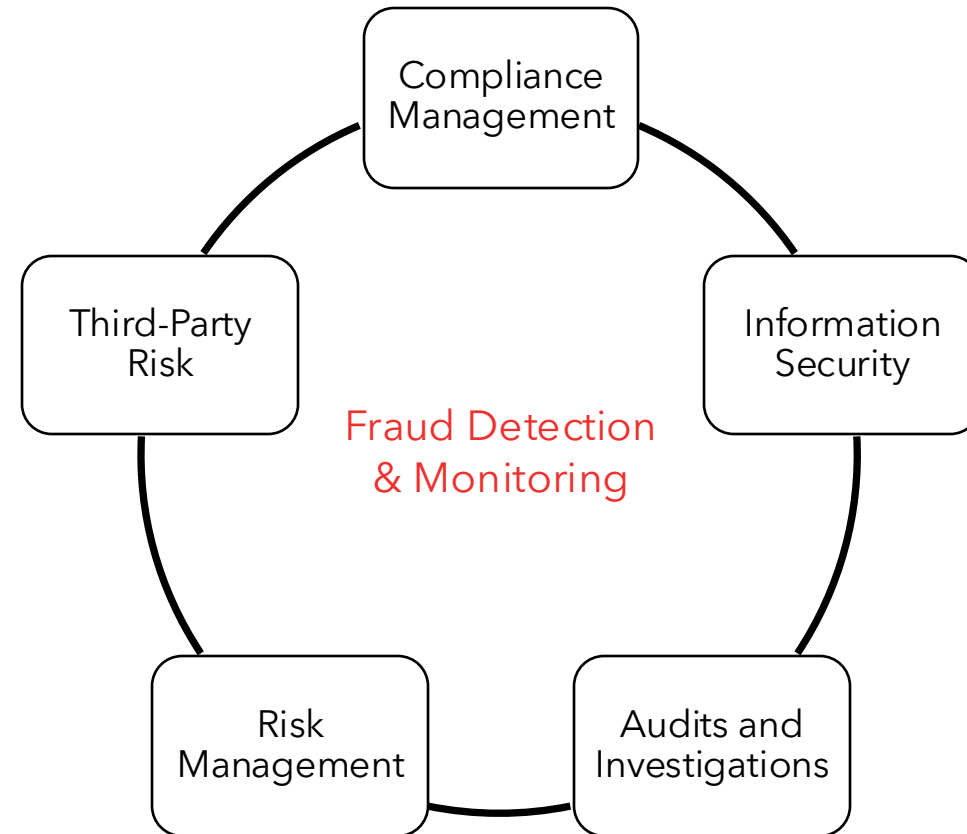
General Challenges for Organizations
Disparate Data Sources

Challenges

- Increased data siloes
- Difficulties in accessing reliable and consistent information
- Makes effective decision-making difficult
- Hinders effective collaboration between different departments, educators, and staff members
- Disparate reporting

Potential Solutions

- Improve data integration and quality
- Create data dictionaries
- Consolidate solutions
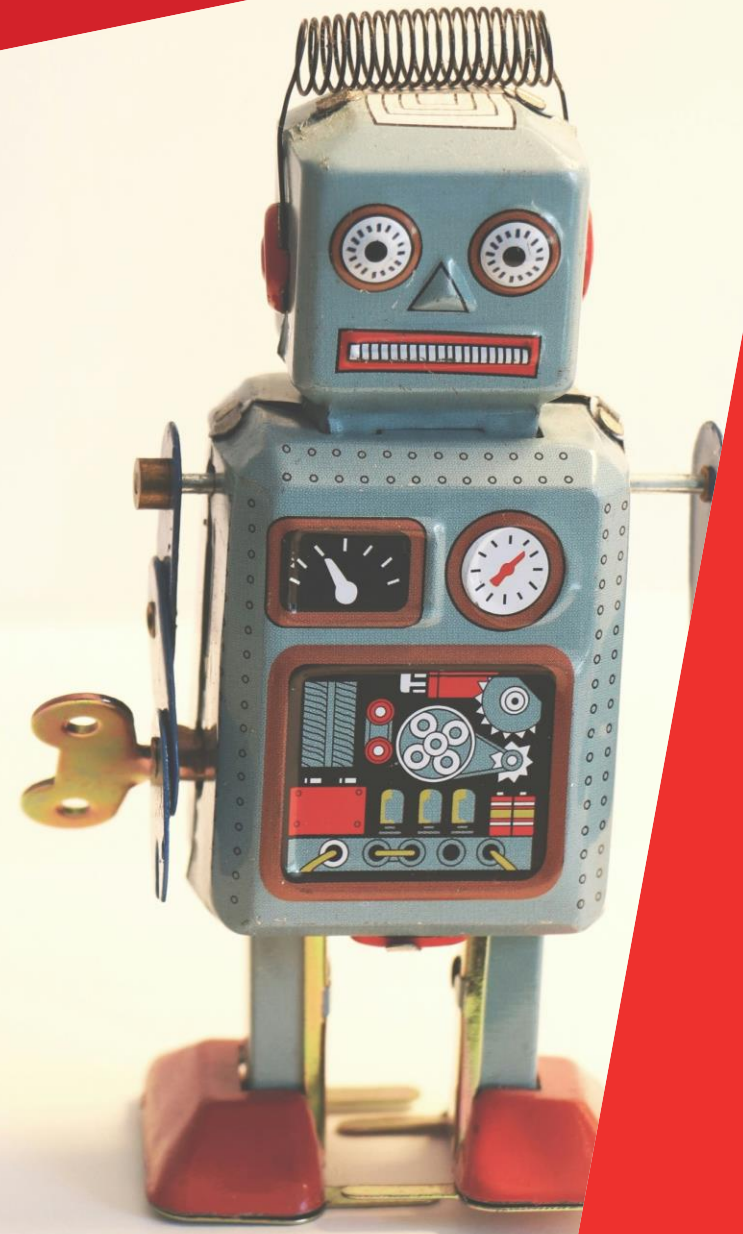
What Do the Standards Say?
IIA IPPF

Diligent

Updated IIA IPPF Standards

What changed?

- New IIA IPPF standards emphasize the importance of a continuous risk assessment in internal audit functions.

- Standards see risk not only as barriers but opportunities to achieve objectives.

- Updated standards emphasize greater reliance on technology integration in auditing processes.

- Encourages auditors to use technology for risk assessments, data analysis, and continuous monitoring to enhance audit efficiency and effectiveness.

Diligent

Key Areas for Collaboration
ERM and Audit

Diligent

Key Areas where Auditors and ERM can Collaborate

Governance and Independence

- **Independence:** Auditors offer objective assurance while ERM managers are responsible to facilitate risk ownership in the business units of an organization

- **Risk Alignment:** Risk based auditing allows auditors to align their audit plans to ERM risk assessments and prioritize the highest risks affecting an institution

- **Continuous Monitoring:** Use real-time dashboards for fraud, cybersecurity, and compliance risks

- **Integrate Information:** Share risk data across the institution to prevent data siloes between audit and ERM

- **Regulatory Compliance:** Ensure adherence to IIA standards and the COSO framework (or other risk frameworks)

Diligent

Real-Time Dashboards

Example

ERM Reporting

Dashboards allow for the consolidation of risk data from different parts of the organization, providing both risk and audit teams with a centralized view of emerging threats, control effectiveness, and mitigation strategies. This transparency:

- Helps the risk team identify and assess evolving risks

- Enables the audit team to evaluate whether internal controls are effectively managing those risks
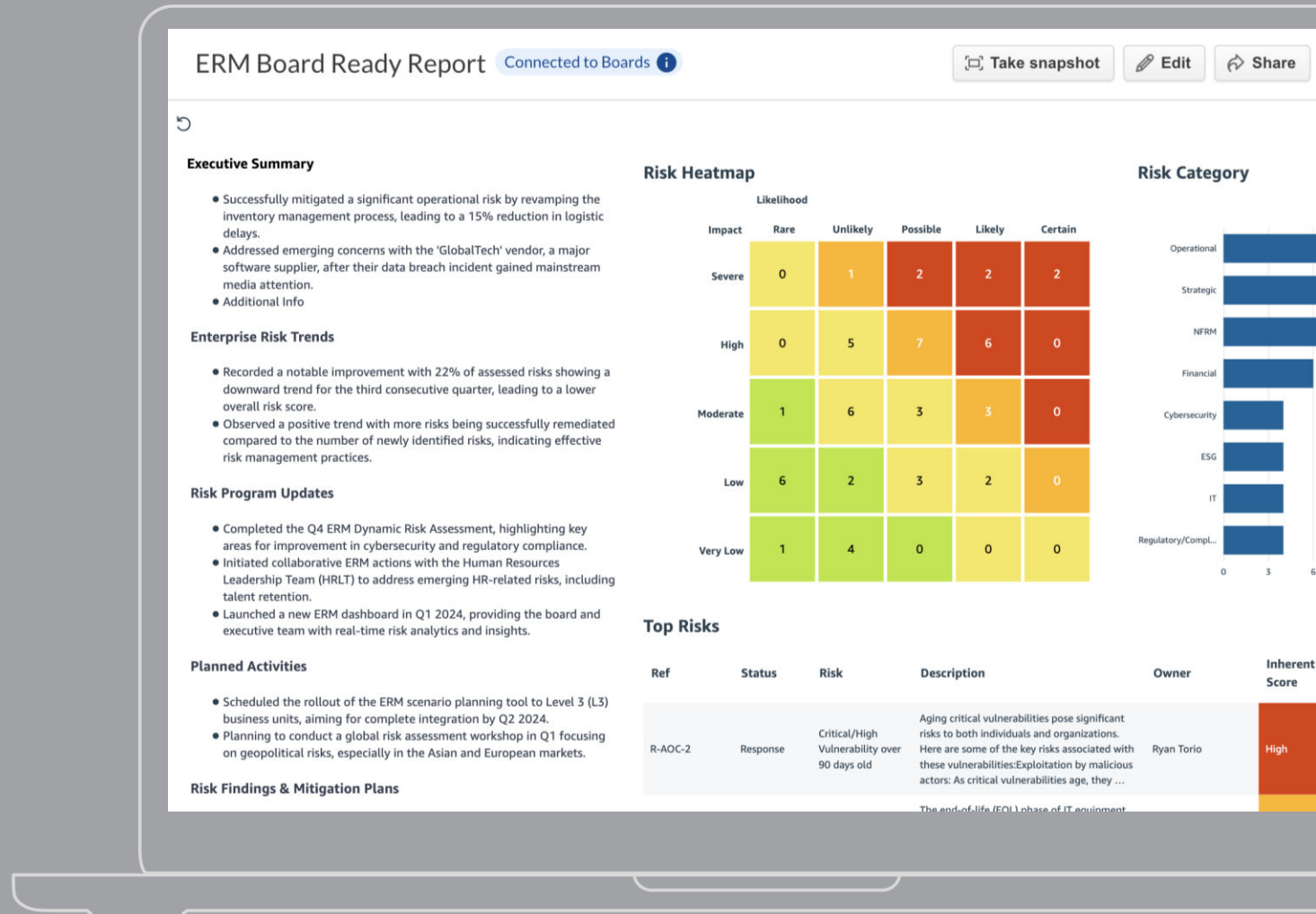
Polling Question #2

Have you increased your efforts in collaborating with risk owners to detect fraud?

a. Yes
b. No
c. I don't know
d. We don't have problems with fraud

Changes in Higher Ed

More data leading to informed decisions

How Can a Continuous Risk Assessment Help?

- Early detection of fraud patterns

- Pro-active risk mitigation

- Continuous monitoring and alerts

- Strengthens internal controls

- Supports data-driven fraud prevention strategies

- Establishes employee awareness and ethical culture

- Auditors can conduct a continuous risk assessment to inform their Annual Audit Plan

- Risk Managers conduct continuous risk assessment to inform their 2nd line of defense duties and the strategic risks of an organization.

- Both can collaborate on these tasks

Integrating a Continuous Risk Assessment with Internal Controls Monitoring

2nd Line of Defense

What can be done?

- Ongoing review of controls to monitor design and functioning of the controls
- Monitoring becomes more targeted when integrated with a continuous risk assessment

  - Real-time detection of control deficiencies

  - Prompt remediation

  - Use tools to automate processes

  - Quick feedback enabling continuous improvement
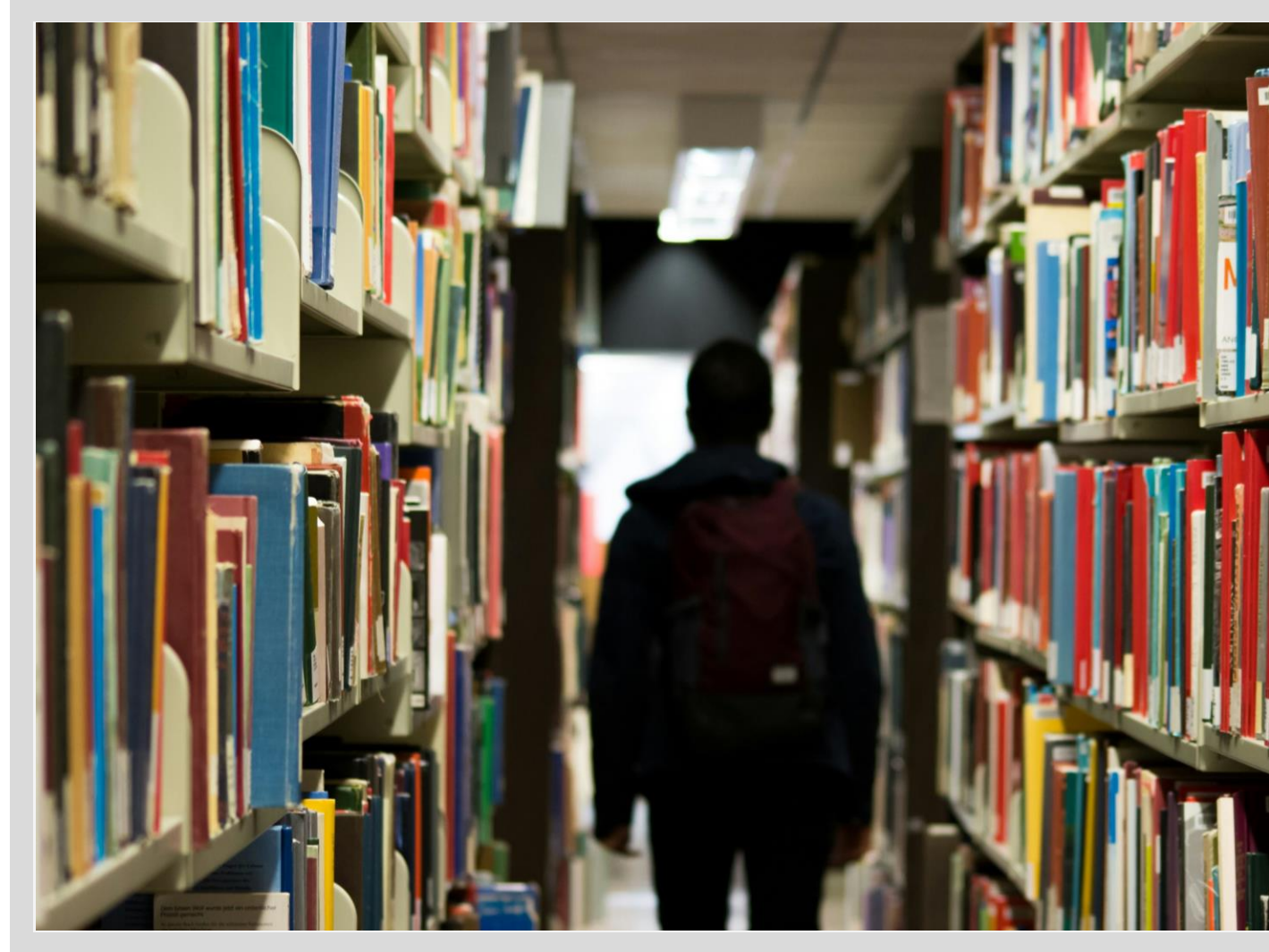
Combined Assurance for Organizational Governance

Not mandated but Encouraged

Advantages:

- Assurance mapping
- Enhanced governance and monitoring
- Reduced duplication of efforts

Disadvantages:

- Auditors may observe variations of quality in the work of different assurance providers
- Different assessments/ interpretations of severity of risks
- Lack of objectivity among assurance providers
- Perception of lack of independence of internal audit

Research and Grant Fraud Indicators

Example

Diligent

Research & Grant Fraud Indicators

Reputational and Financial Damage to the Institution

Conflict of Interest: Use funds for personal expenses or non-research related expenses

- Analyze detailed expenditure data for patterns of non-research related spending

- Unusual spending categories

- High personal expense amounts

- Geographically inconsistent spending

- Discrepancy between expense justification and actual spending

Research & Grant Fraud Indicators

Reputational and Financial Damage to the Institution

- **Data Fabrication:** Researchers submit false or plagiarized information

- **Misuse of Research Funds:** Undisclosed relationships between researchers and external people or organizations

Procurement and Vendor Fraud
Example

Diligent

Example
Hacking Into Vendor's Computer

Thieves steal $107,000 from UCF in sophisticated hacking scheme

WUFT | By Kai Johnsen | Fresh Take Florida
Published December 17, 2024 at 3:15 PM EST

Fresh Take Florida / State University System

Source: Thieves steal $107,000 from UCF in sophisticatedhacking scheme | WLRN

Procurement & Vendor Fraud

Cause: Lack of oversight of vendor contracts

Examples:

- **False or inflated invoices:** Making payments to nonexistent vendors or overpaying for services; fake invoices.

- **Conflicts of interest:** Higher Ed staff awarding contracts to relatives or friends or accepting bribes from vendors.

- **Kickbacks:** Vendor and employee working together on fraud. Not receiving agreed-upon number of goods/ overbilling.

- **Unauthorized spending:** Purchase of non-educational items with grant or institutional funds (Could be improper payment or fraud)

What Can Be Done From the Audit Side?

- Conduct surprise audits
- Continuous auditing
- Review policies and procedures related to vendor management
  - Regularly review vendor information and contracts
  - Review contract requirements
- Assess if segregation of duties is working

Procurement & Vendor Fraud

Auditors

Conduct Vendor Audits: Include a right-to-audit clause in vendor contracts

- Use analytics to detect unusual patters around transaction volumes, payment frequencies, and vendor information.

- **Example:** Use cross-referencing of information to identify fake vendors submitting fictitious invoices

- **Example:** Identify irregularities associated with employee vendor collusion where a legitimate vendor submits inflated or duplicate invoices. Such as identical purchase numbers, descriptions, amounts, dates etc.

- **Red Flag:** Unusual close association with a vendor

What Can Be Done from the Risk Side?

- Continuously monitor internal controls and check for control failures

- Establish tone at the top that drives all risk owners to feel responsible for the process

- Conduct a continuous risk assessment

  - A regular evaluation of potential risks of an organization

  - Understanding the risk landscape for the entire organization and the emergence of new risks

  - Periodic fraud risk assessments

- **Integrate continuous risk assessment information into ERM program**

Polling Question #3

Are you conducting a continuous risk assessment?

a. Yes
b. No
c. I don't know

Diligent

Leveraging Data to Stay Informed
Proactive Approach

Diligent

"Proactive data monitoring was associated with 52% lower losses and frauds detected in half the time."

Association of Certified Fraud Examiners

Diligent

What Can Data Do for You?

- Review 100% of data for indicators of fraud
- Automate tasks to increase resource capacity
- Quickly respond to identified fraud real time

Types of Analysis

Ad Hoc/Sampling:

- Manual
- Time Consuming
- Element of Human Error

Continuous:

- 100% Coverage
- Real time notifications
- Quickly covers large volumes of data

Diligent

No Process

No data analytic program exists today; rely on canned reports

Adhoc / Manual

Focuses on ad-hoc/manual testing for both process and risk-based analysis

Repeatable

Processes are now repeatable in a DA tool but still require manual action/execution

Automated

Processes are automated in an RDA/RPA tool and require little to no manual action

Continuous

Investigation and remediation of DA program analysis now part of the overall process. Meta data of program efficiency reportable

Diligent

No Process

No data analytic program exists today; rely on canned reports

1

Adhoc / Manual

Focuses on ad-hoc/manual testing for both process and risk-based analysis

Repeatable

Processes are now repeatable in a DA tool but still require manual action/execution

Automated

Processes are automated in an RDA/RPA tool and require little to no manual action

Continuous

Investigation and remediation of DA program analysis now part of the overall process. Meta data of program efficiency reportable

No Process

No data analytic program exists today; rely on canned reports

1

Adhoc / Manual

Focuses on ad-hoc/manual testing for both process and risk-based analysis

2

Repeatable

Processes are now repeatable in a DA tool but still require manual action/execution

Automated

Processes are automated in an RDA/RPA tool and require little to no manual action

Continuous

Investigation and remediation of DA program analysis now part of the overall process. Meta data of program efficiency reportable

No Process

No data analytic program exists today; rely on canned reports

1

Adhoc / Manual

Focuses on ad-hoc/manual testing for both process and risk-based analysis

2

Repeatable

Processes are now repeatable in a DA tool but still require manual action/execution

3

Automated

Processes are automated in an RDA/RPA tool and require little to no manual action

Continuous

Investigation and remediation of DA program analysis now part of the overall process. Meta data of program efficiency reportable

No Process

No data analytic program exists today; rely on canned reports

1

Adhoc / Manual

Focuses on ad-hoc/manual testing for both process and risk-based analysis

2

Repeatable

Processes are now repeatable in a DA tool but still require manual action/execution

3

Automated

Processes are automated in an RDA/RPA tool and require little to no manual action

4

Continuous

Investigation and remediation of DA program analysis now part of the overall process. Meta data of program efficiency reportable

1 No Process — No data analytic program exists today; rely on canned reports

2 Adhoc / Manual — Focuses on ad-hoc/manual testing for both process and risk-based analysis

3 Repeatable — Processes are now repeatable in a DA tool but still require manual action/execution

4 Automated — Processes are automated in an RDA/RPA tool and require little to no manual action

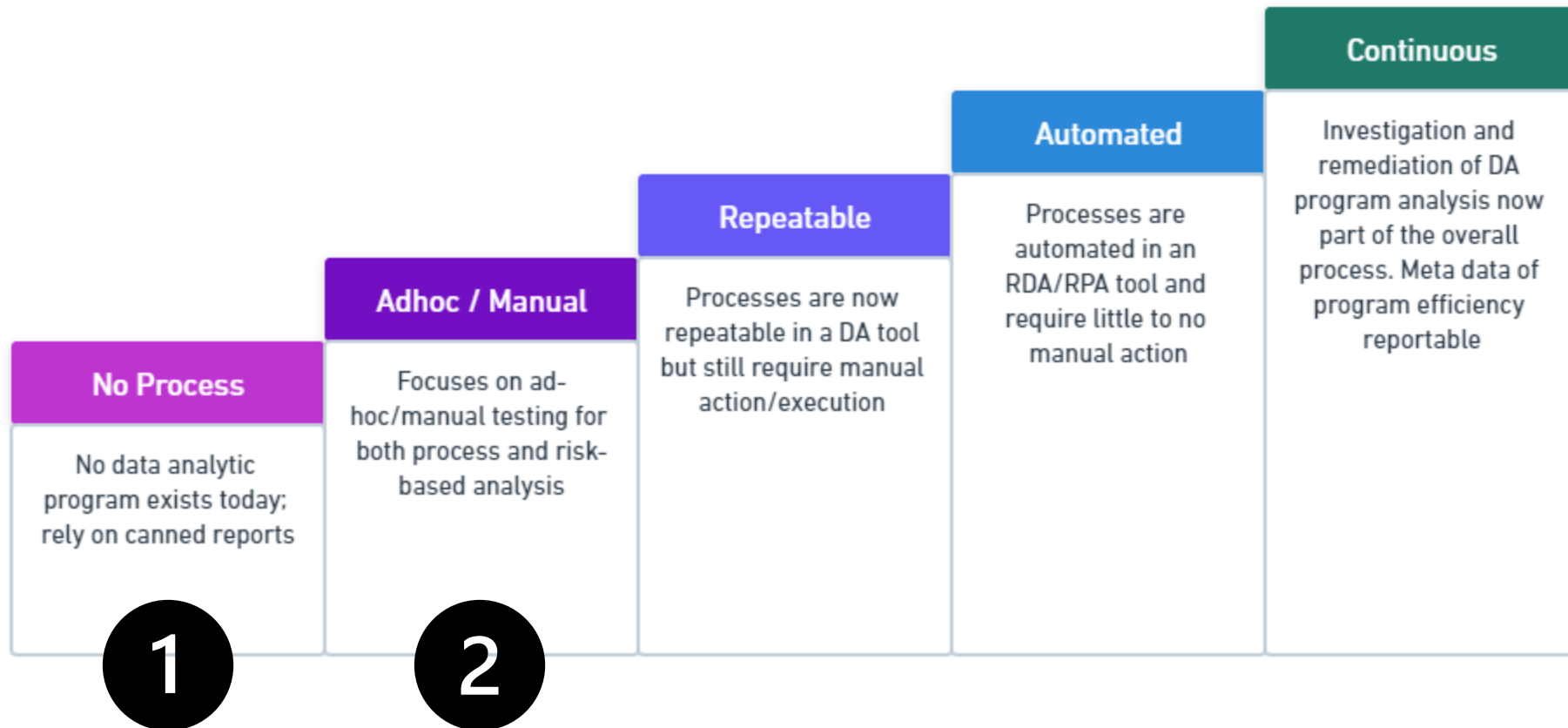**5** Continuous — Investigation and remediation of DA program analysis now part of the overall process. Meta data of program efficiency reportable
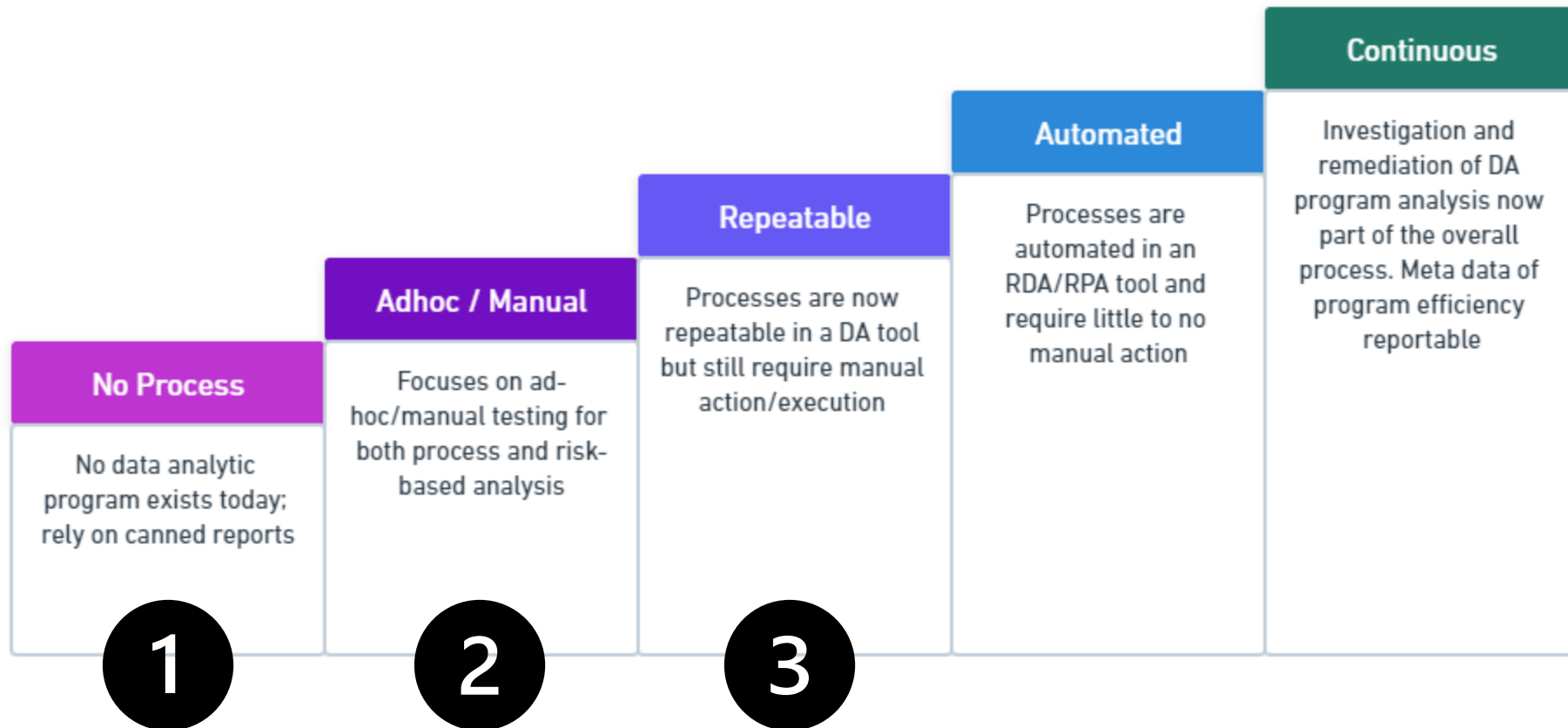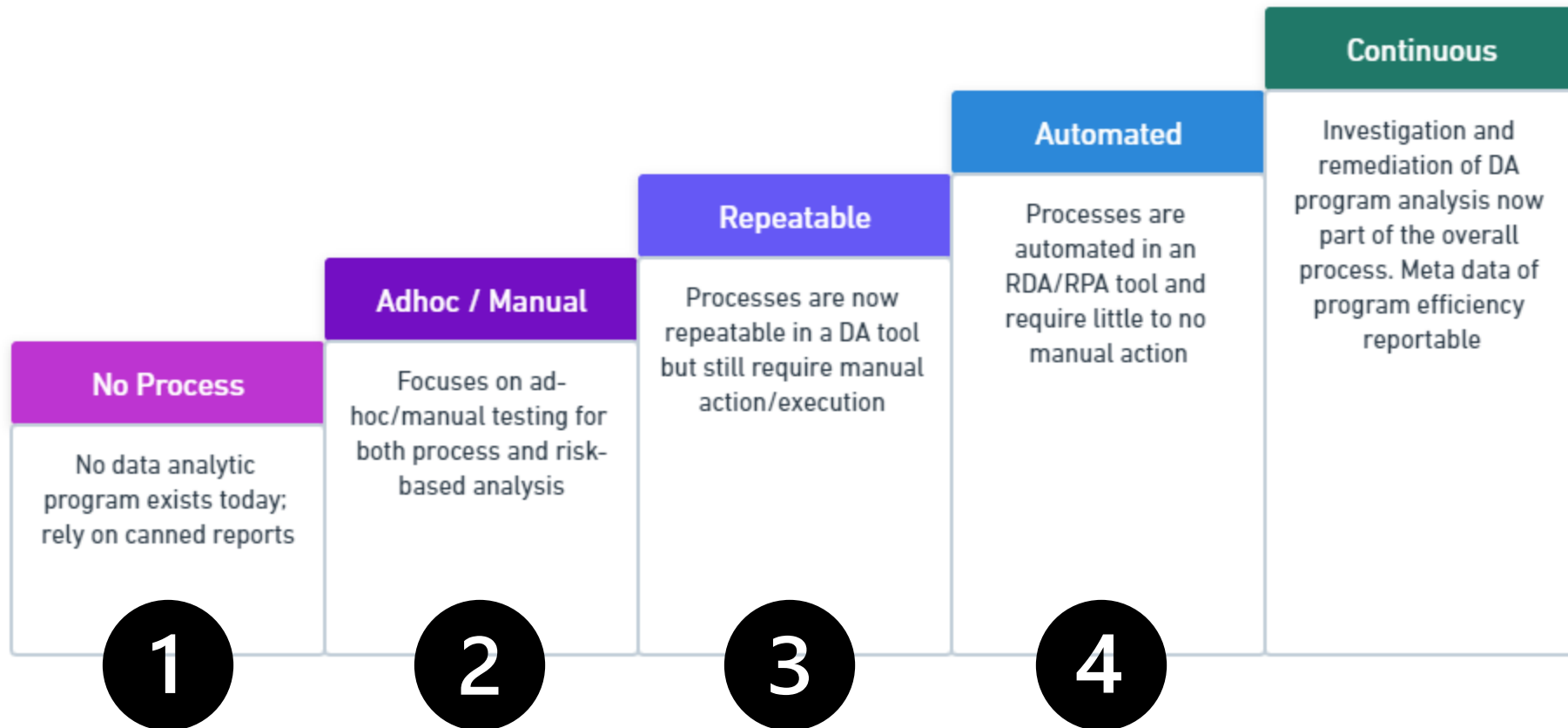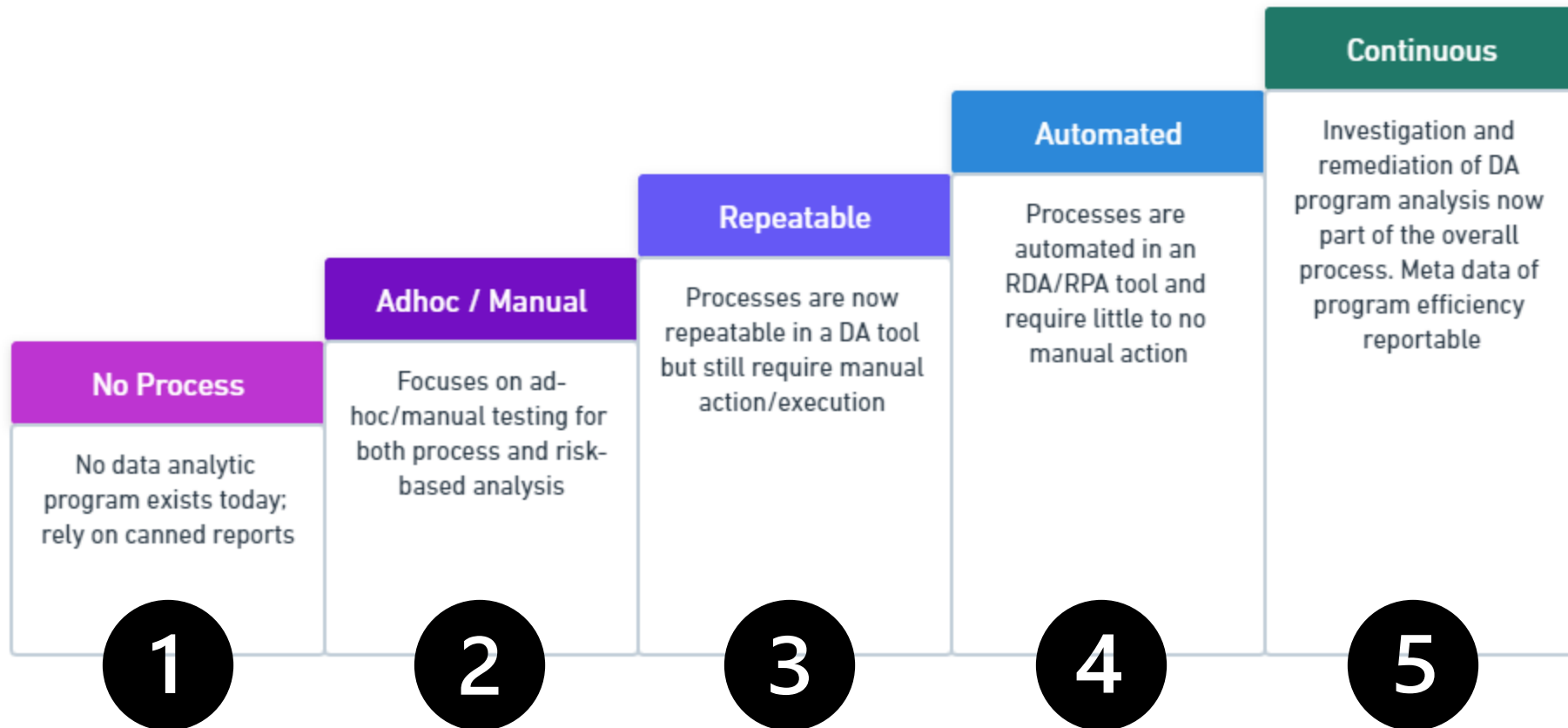
Introduction to Continuous Monitoring
New Era of Risk Monitoring and Mitigation

Diligent

The ongoing process of monitoring and assessing internal controls within an organization to ensure compliance, efficiency, and risk mitigation

Definition of CCM

Diligent

Significance of CCM
Active Fraud Mitigation

1. **Early Detection of Fraudulent Activities**

   • CCM continuously analyzes transactions, user behavior, and control effectiveness, allowing organizations to identify suspicious patterns and anomalies before they escalate into significant fraud incidents.

2. **Reducing the Fraud Triangle (Opportunity, Rationalization, Pressure)**

   • By minimizing opportunities for fraud through automated controls, CCM discourages fraudulent behavior. If employees know that controls are actively monitored, the risk of detection increases, reducing the likelihood of misconduct.

3. **Strengthening Internal Controls**

   • Traditional audits and periodic reviews may miss real-time fraud, but CCM ensures that internal controls are enforced consistently, preventing gaps where fraud can occur.

Diligent
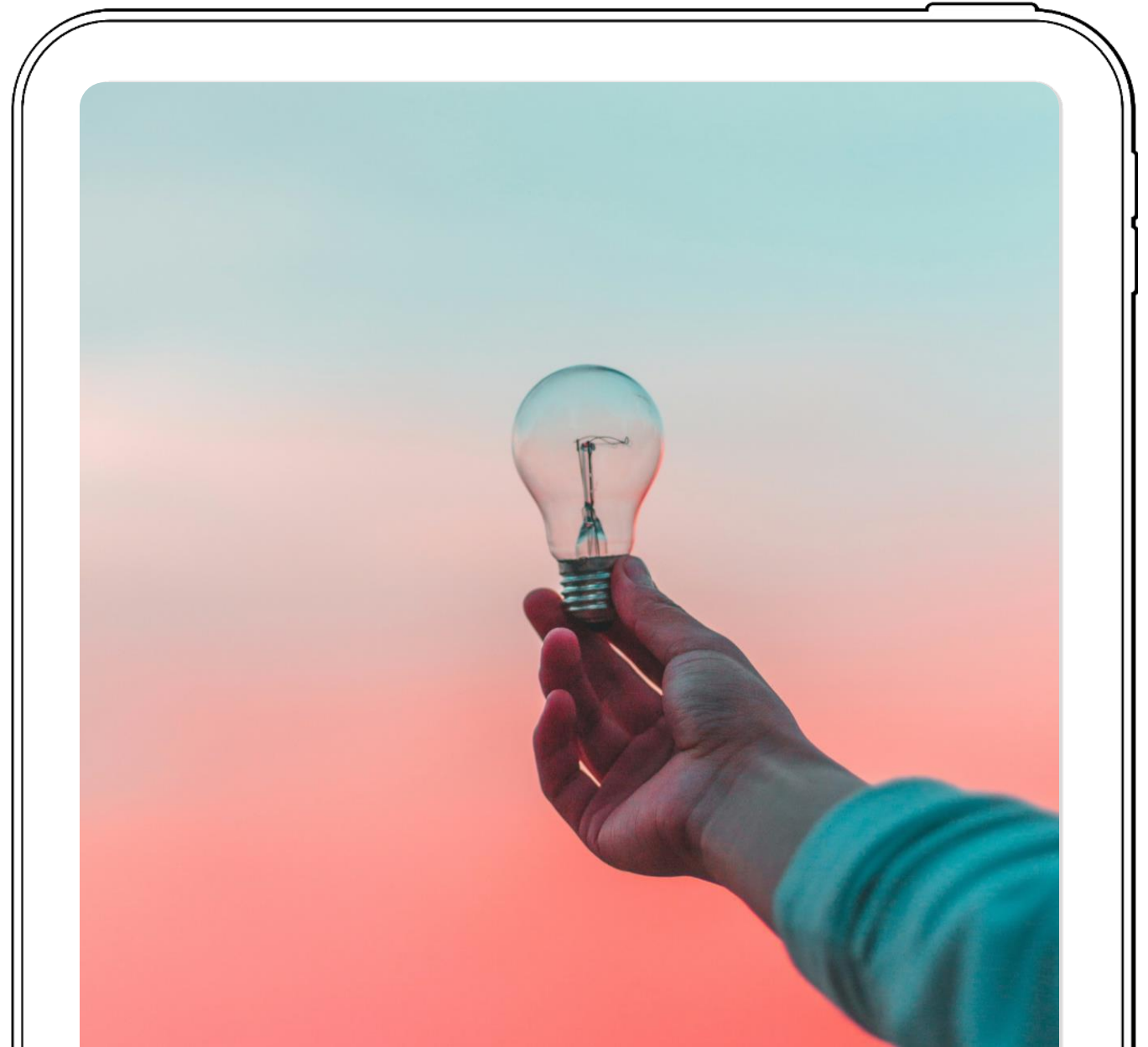
Significance of CCM
Active Fraud Mitigation Continued

4. **Compliance with Regulations and Standards**

    - Many industries require strict compliance with financial regulations (e.g., SOX, GDPR, COSO). CCM helps ensure compliance by continuously verifying adherence to policies, reducing regulatory risks.

5. **Cost Savings and Efficiency**

    - Proactively preventing fraud through CCM reduces the need for costly forensic investigations and legal proceedings after fraud has already occurred. It also optimizes internal audit efforts by automating control testing.

6. **Data-Driven Fraud Prevention**

    - By leveraging machine learning, AI, and analytics, CCM can predict potential fraud risks and flag irregularities based on trends, allowing organizations to address vulnerabilities proactively.
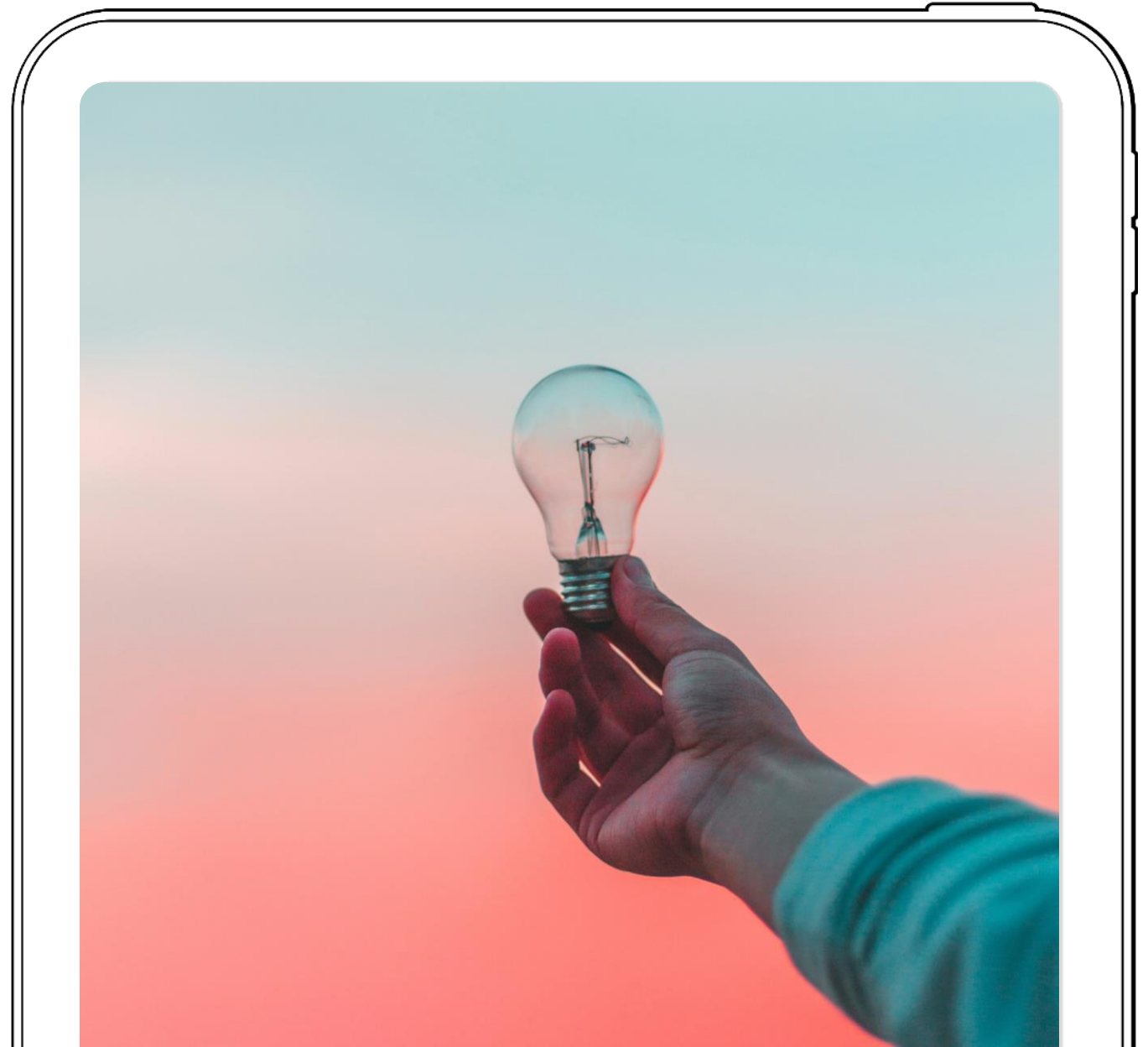
Key Components

Automated Data Collection

- Collect data from various sources, such as ERP systems, databases, logs, assets, and IT security solutions in an automated and real-time manner.
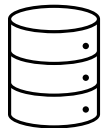
Rule Engine

- Define specific rules and thresholds that indicate control violations or anomalies.

- Immediate notification and action of potential issues.

Analytics and Reporting

- Analyze large datasets, detect patterns, and generate insightful reports.

Remediation Workflow

- Establish a process for addressing and remediating control deficiencies once identified.

- Ensuring that issues are addressed systematically and in a timely manner.

Continuous Improvement

Ongoing assessment and enhancement of CCM processes to adapt to evolving risks and business needs.

Polling Question #4

Are you performing any continuous monitoring activities?

a. Yes
b. No
c. I don't know

Continuous Audit Analytics

Example

Purchase Card Audit

Leverage analysis of purchase card data to continuously monitor against fraud related procedures / controls

1. Perform analysis on purchase card data to determine instances where transactions exceeded a pre-defined threshold

Continuous Audit Analytics

Example

Purchase Card Audit

Leverage analysis of purchase card data to continuously monitor against fraud related procedures / controls

1. Perform analysis on purchase card data to determine instances where transactions exceeded a pre-defined threshold
2. Define a metric (key performance / key risk indicator) based on the outcomes of the analysis

Metrics 1

\# OVER THRESHOLD   KPI

113

Continuous Audit Analytics

Example

Purchase Card Audit

Leverage analysis of purchase card data to continuously monitor against fraud related procedures / controls

1. Perform analysis on purchase card data to determine instances where transactions exceeded a pre-defined threshold
2. Define a metric (key performance / key risk indicator) based on the outcomes of the analysis
3. Set thresholds that define control success / failure criteria based on the defined metric

| Metric | # Over Threshold ▾ |

 # OVER THRESHOLD [KPI]

113

| less than ▾ | < | 120 |

= No Issues

| greater than or equal to | ≥ | 120 |

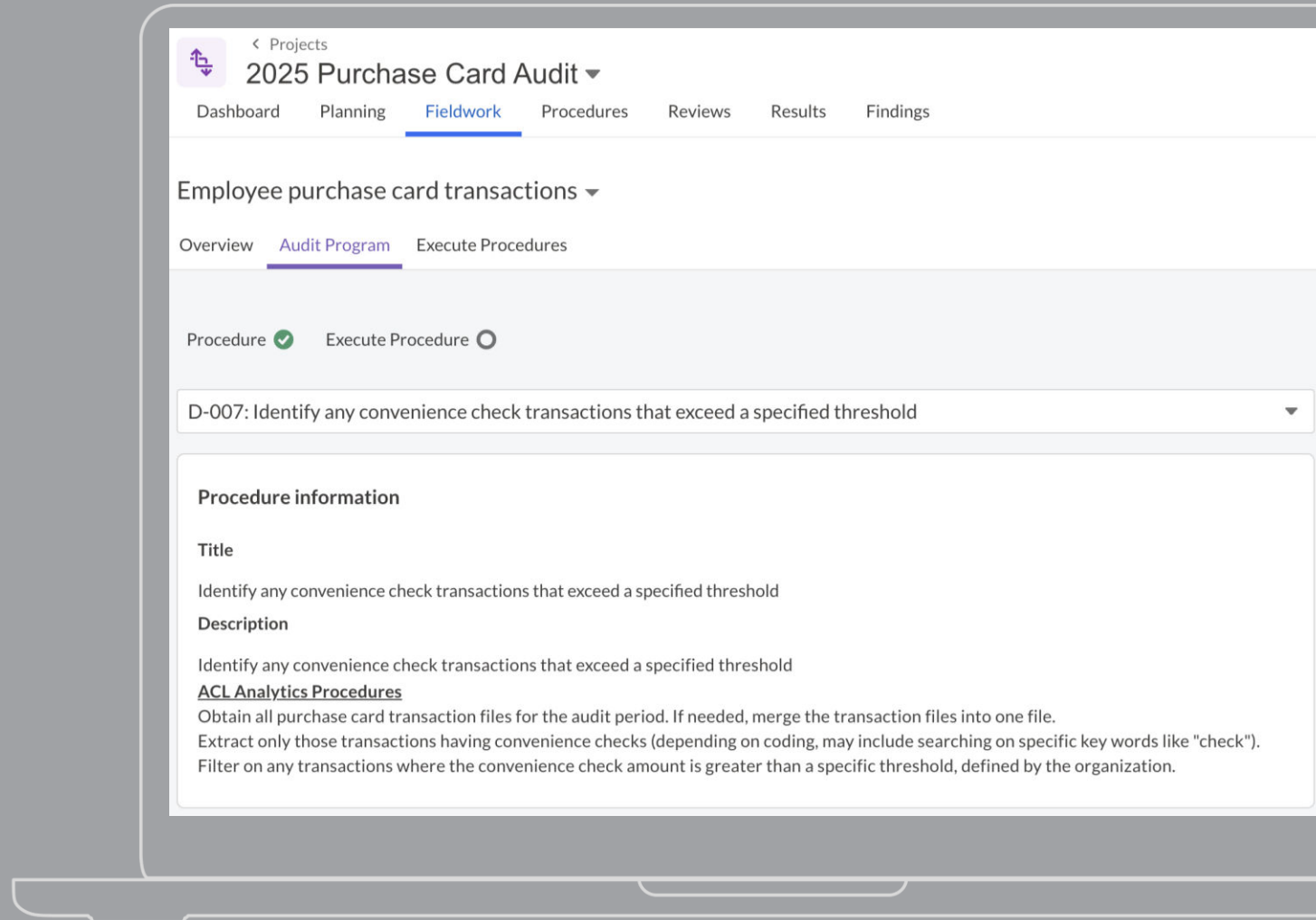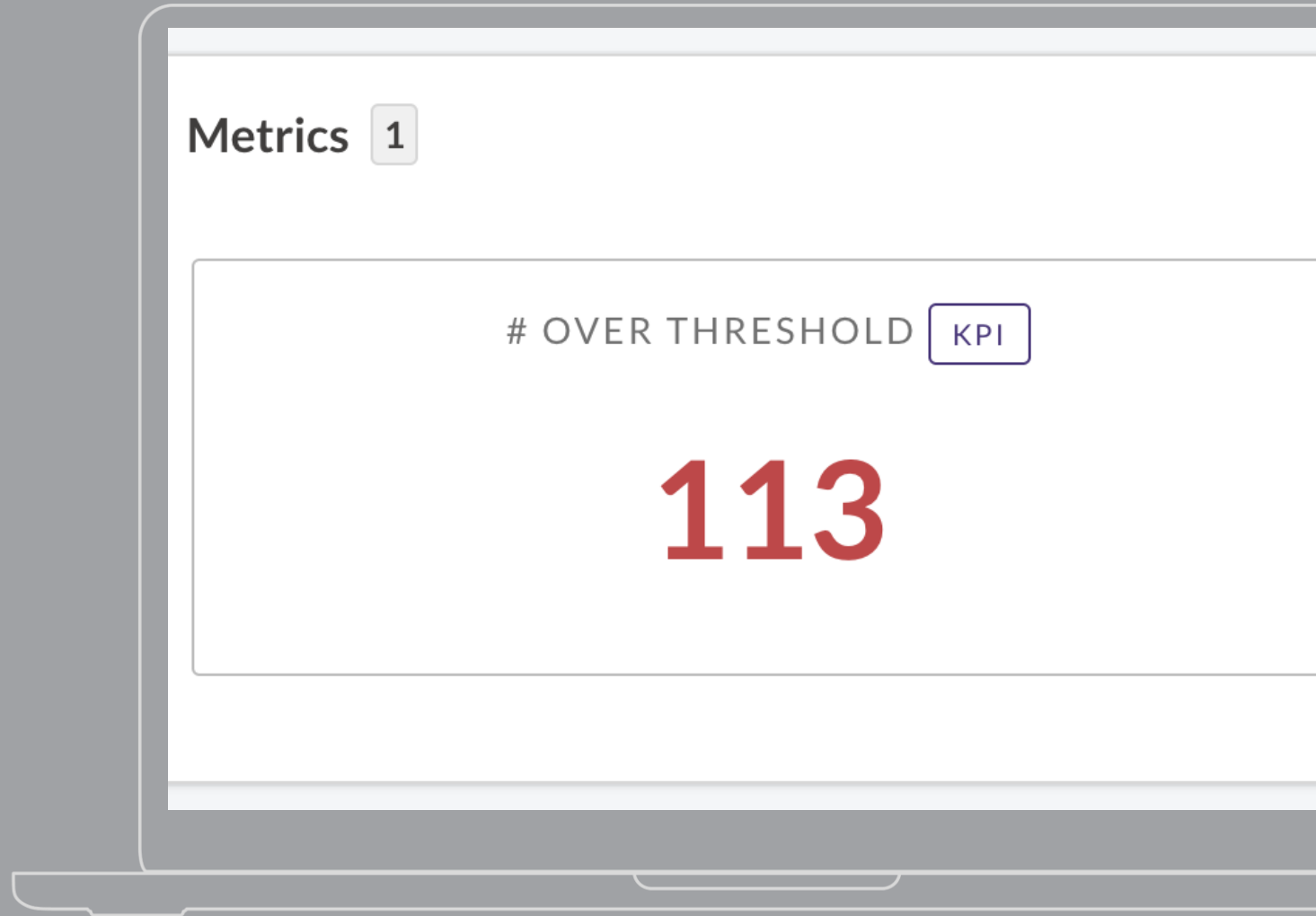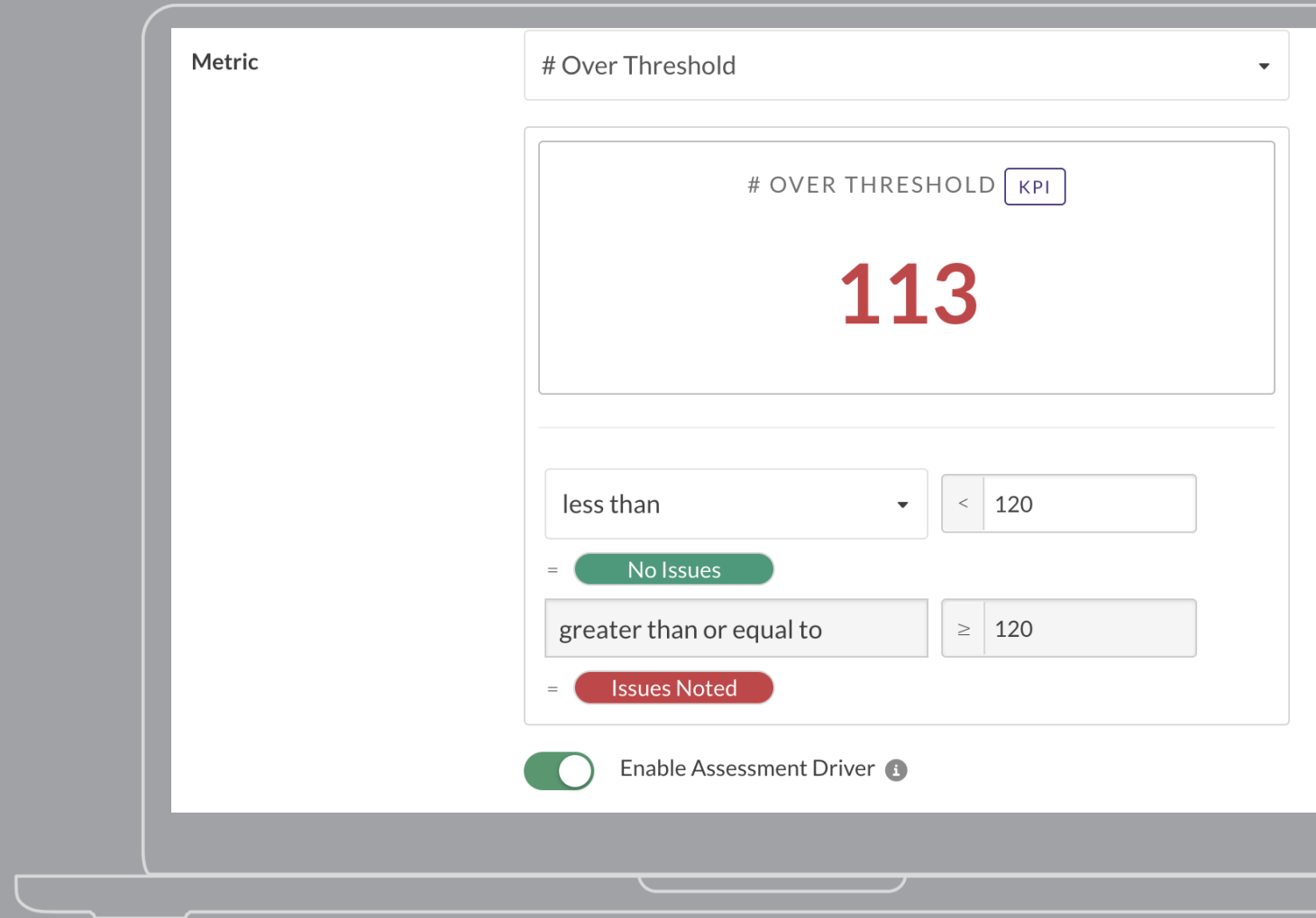= Issues Noted

⬤ Enable Assessment Driver ⓘ

Continuous Audit Analytics

Example

Purchase Card Audit

Leverage analysis of purchase card data to continuously monitor against fraud related procedures / controls

1. Perform analysis on purchase card data to determine instances where transactions exceeded a pre-defined threshold

2. Define a metric (key performance / key risk indicator) based on the outcomes of the analysis

3. Set thresholds that define control success / failure criteria based on the defined metric

4. Inform real-time dashboards on control monitoring outcomes

| Risk Details | Compliance Tests | Financial Exposure |

Compliance Test Details

Test Reference	Test Description	Testing Type	2023	2022	2020
T1	Exceeds Single Transaction Limit	Full Population	100%	100%	100%
T10	Purchase Date Before Approval Date	Sample Selection	80%	62.14%	100%
T11	Segregation of Duties	Sample Selection	90%	82.69%	88.12%
T12	Cardholder Reconciliation Verification	Sample Selection	100%	100%	0%
T13	Supporting Documentation	Sample Selection	100%	100%	98%
T14	Valid Receipts	Sample Selection	100%	100%	97.6%
T15	Duplicate Transactions	Sample Selection	100%	100%	100%
T2	Exceeds Monthly Credit Limit	Full Population	100%	100%	100%
T3	Purchase Day = Leave Day	Full Population	100%	100%	100%
T4	Weekend/Holiday Transactions	Full Population	100%	100%	100%
T5	Prohibited MCC Transactions	Full Population	100%	100%	100%
T6	Split Purchases	Full Population	100%	99.75%	99.75%
T7	State Sales Tax	Full Population	100%	100%	100%
T8	Proper WORKS Approvals	Full Population	100%	99%	100%
T9	Gift Card/Cash Advance	Full Population	100%	100%	100%

Compliance Average 2023	Compliance Average 2022	Compliance Average 2020
↑ 98.00%	↑ 96.24%	↑ 92.23%

Continuous Risk Assessment Analytics
Example

Increases in Improper Payments

Leverage analysis of financial ERP data to continuously monitor against fraud related risks

1. Perform analysis on financial ERP data to surface insights that can be used as input into risk assessment activities

Increases in Improper Payments ✎

Acceptance ▾ | Sharing ▾ | ✕

Inherent Risk Heat	Residual Risk Heat
13.1%	4.75%
Score: 13.0	Score: 4.7

Description ✎

This might include overpayments, duplicate payments, payments without proper authorization, or payments to ineligible recipients. Assess the potential impact of improper payments on the organization in terms of financial losses, reputation damage, legal consequences, and regulatory compliance. Implement monitoring systems and controls to detect irregularities in payment processes. This can include regular audits, data analytics, and automated tools to identify anomalies or patterns indicative of improper payments.

Details Metrics Assessment Treatment Assurance Discussion Activities

Risk Owner | Lucy Liu

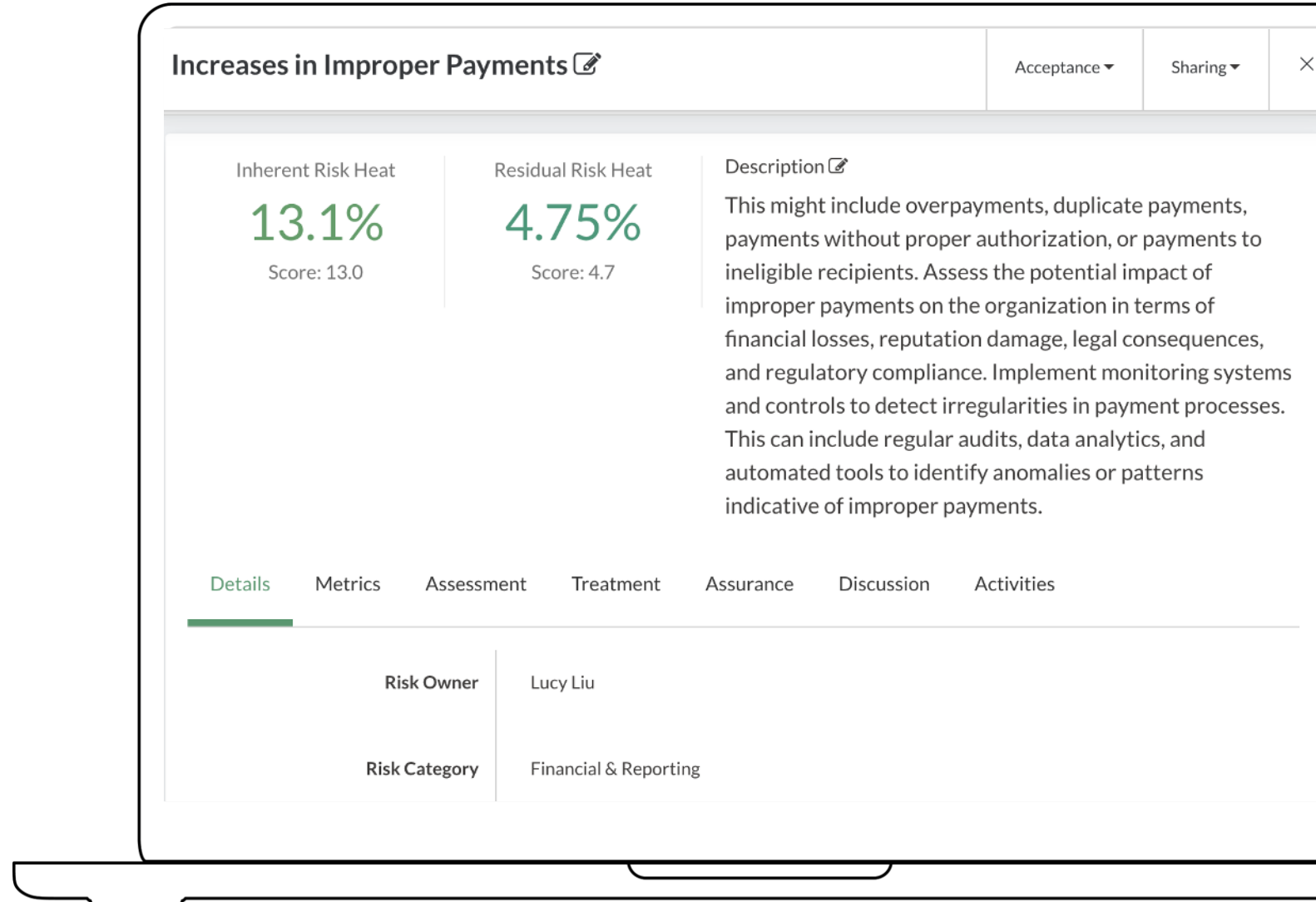Risk Category | Financial & Reporting

Continuous Risk Assessment Analytics

Example

Increases in Improper Payments

Leverage analysis of financial ERP data to continuously monitor against fraud related risks

1. Perform analysis on financial ERP data to surface insights that can be used as input into risk assessment activities
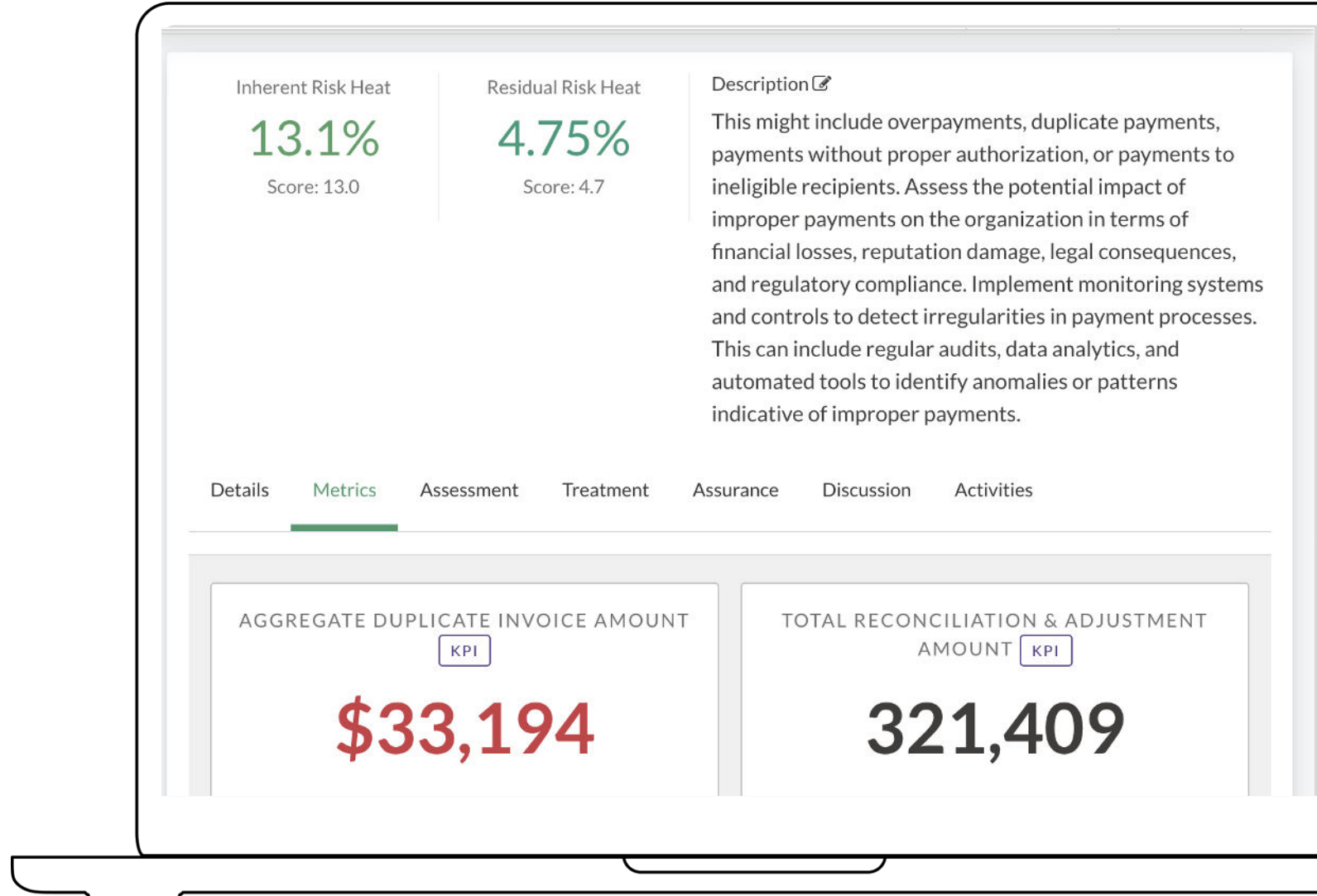2. Define a metric (key performance / key risk indicator) based on the outcomes of the analysis

Inherent Risk Heat

13.1%

Score: 13.0

Residual Risk Heat

4.75%

Score: 4.7

Description ✎

This might include overpayments, duplicate payments, payments without proper authorization, or payments to ineligible recipients. Assess the potential impact of improper payments on the organization in terms of financial losses, reputation damage, legal consequences, and regulatory compliance. Implement monitoring systems and controls to detect irregularities in payment processes. This can include regular audits, data analytics, and automated tools to identify anomalies or patterns indicative of improper payments.

Details   Metrics   Assessment   Treatment   Assurance   Discussion   Activities

AGGREGATE DUPLICATE INVOICE AMOUNT [KPI]

$33,194

TOTAL RECONCILIATION & ADJUSTMENT AMOUNT [KPI]

321,409

Continuous Risk Assessment Analytics

Example

Increases in Improper Payments

Leverage analysis of financial ERP data to continuously monitor against fraud related risks

1. Perform analysis on financial ERP data to surface insights that can be used as input into risk assessment activities

2. Define a metric (key performance / key risk indicator) based on the outcomes of the analysis
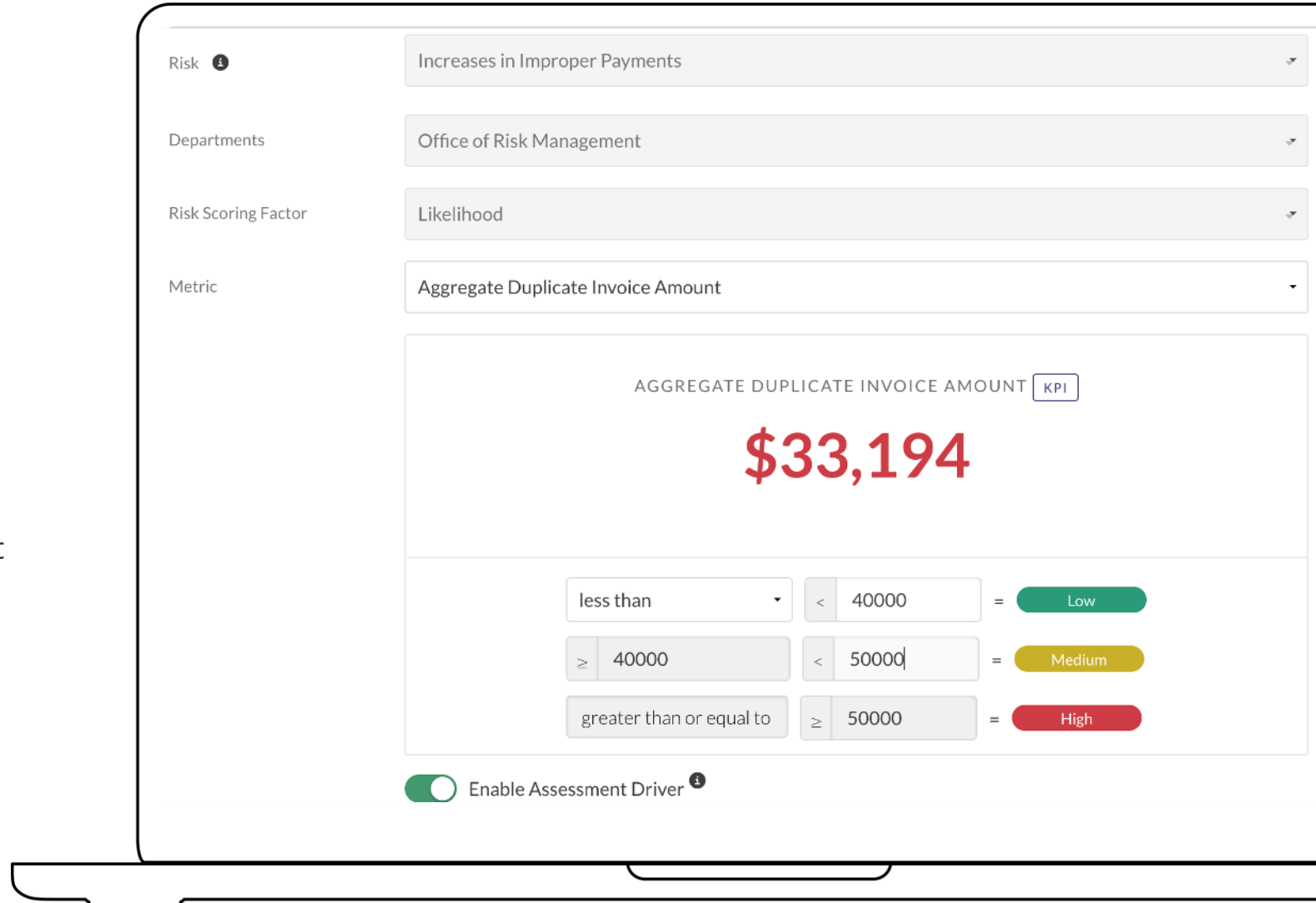
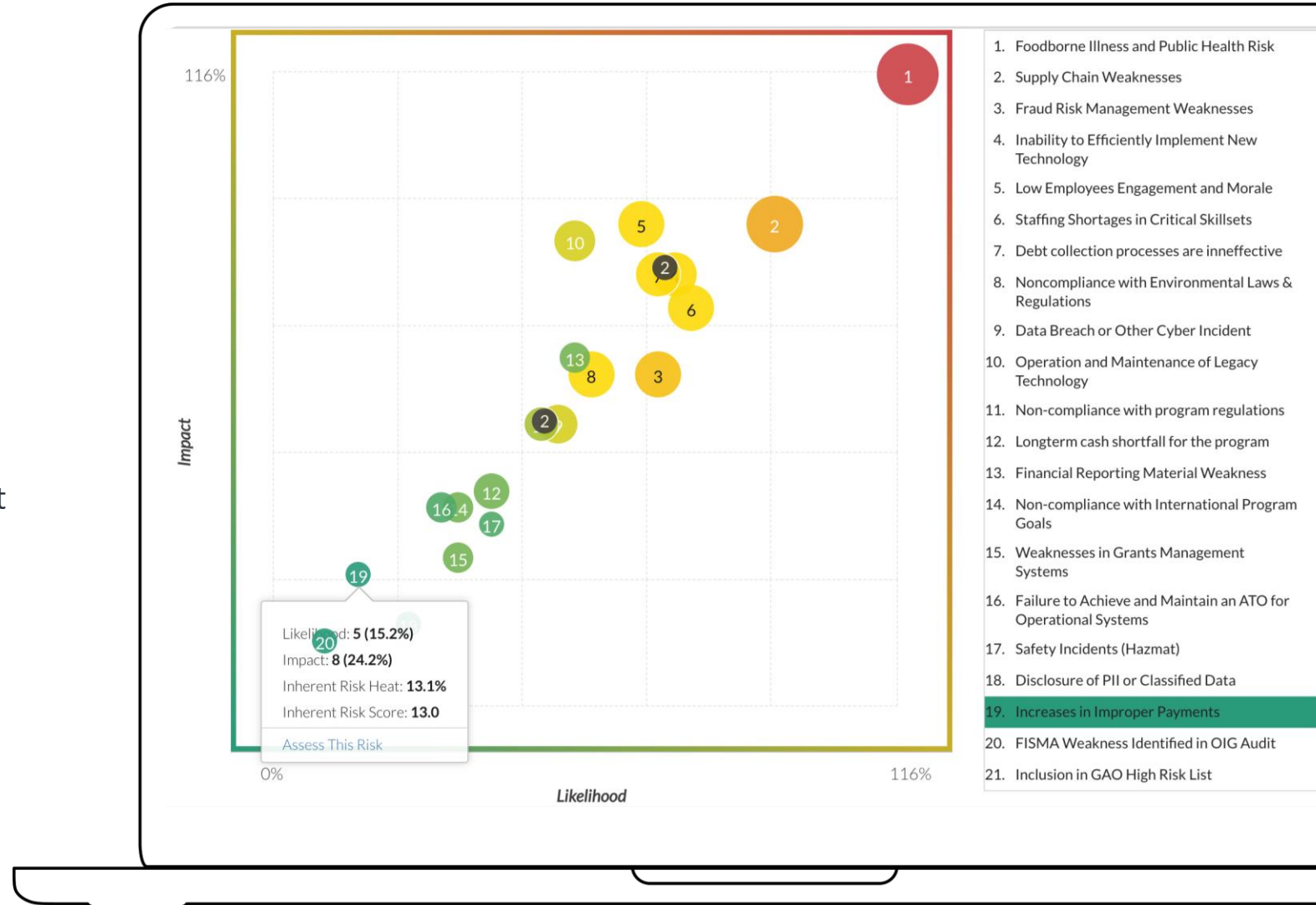3. Set thresholds that define risk scoring based on the defined metric

Risk ⓘ   Increases in Improper Payments

Departments   Office of Risk Management

Risk Scoring Factor   Likelihood

Metric   Aggregate Duplicate Invoice Amount

AGGREGATE DUPLICATE INVOICE AMOUNT [KPI]

$33,194

less than	< 40000	= Low
≥ 40000	< 50000	= Medium
greater than or equal to	≥ 50000	= High

Enable Assessment Driver ⓘ

Continuous Risk Assessment Analytics

Example

Increases in Improper Payments

Leverage analysis of financial ERP data to continuously monitor against fraud related risks

1. Perform analysis on financial ERP data to surface insights that can be used as input into risk assessment activities

2. Define a metric (key performance / key risk indicator) based on the outcomes of the analysis

3. Set thresholds that define risk scoring based on the defined metric

4. Inform real-time dashboards on risk assessment monitoring outcomes

1. Foodborne Illness and Public Health Risk
2. Supply Chain Weaknesses
3. Fraud Risk Management Weaknesses
4. Inability to Efficiently Implement New Technology
5. Low Employees Engagement and Morale
6. Staffing Shortages in Critical Skillsets
7. Debt collection processes are inneffective
8. Noncompliance with Environmental Laws & Regulations
9. Data Breach or Other Cyber Incident
10. Operation and Maintenance of Legacy Technology
11. Non-compliance with program regulations
12. Longterm cash shortfall for the program
13. Financial Reporting Material Weakness
14. Non-compliance with International Program Goals
15. Weaknesses in Grants Management Systems
16. Failure to Achieve and Maintain an ATO for Operational Systems
17. Safety Incidents (Hazmat)
18. Disclosure of PII or Classified Data
19. Increases in Improper Payments
20. FISMA Weakness Identified in OIG Audit
21. Inclusion in GAO High Risk List

Q&A

Diligent

Connect with us!

Follow us on social for the latest audit & ERM resources

Diligent Audit

Katja Freeman

Chris Trepte

Thank You

Diligent

Announcements

Upcoming ACUA Webinars – Save the Date!

Month	Date & Time	Presenter	Topic
March 2025	3/27/25 – 1:00pm EST	Baker Tilly	Sponsored Programs Risk Assessments
April 2025	4/24/25 – 1:00pm EST	Sarah MacCarthy	Navigating Policy Changes in Academia
May 2025	5/22/25 – 1:00pm EST (90-minute webinar)	Nik Henegar	Audit Bots: Revolutionizing Audits with RPA and Macros

Do you have an idea for a webinar? Contact the VLC director at wshinsato@calstate.edu

ACUA
Association of College & University Auditors

Get Involved

Become a Volunteer	Nominate your Colleagues for an ACUA Award	Submit a Conference Proposal
Present a Webinar	Become a Mentor	Write an Article for the College & University Auditor
Write a Kick Starter	Post on Connect ACUA	Share, Like, Tweet & Connect on Social Media

ACUA
Association of College
& University Auditors

Join us for an upcoming webinar