Diligent

Mastering Continuous Control Monitoring: A Strategic Approach for IT Controls

Bio

Chris Trepte, Client Partner

- Chris Trepte is a Client Partner at Diligent who works with and supports clients across Audit, Risk and Compliance teams within the State, Local, and Education Department as well as Federal Government verticals.

- Prior to joining Diligent, Chris had 8+ years of experience at BDO and Protiviti, leading and executing IT consulting engagements encompassing IT General Controls, SOC 2 Readiness, ICFR, SOX and NIST Compliance as well as ad-hoc IT Security reviews.

Diligent

Bio

Alex Fung, Advisory & Consulting Manager

- Alex Fung is an Advisory & Consulting Manager in the Professional Services team at Diligent, mainly focuses on Data Analytics, Automation and Robotics project delivery for 15+ year, managed over 100 implementation projects and worked on over 200 engagement across many industries.

Diligent

Learning Objectives

1. Understand the concept of Continuous Control Monitoring (CCM) with a focus on IT controls.

2. Learn the key principles and components of CCM, including automated data collection, real-time monitoring, and exception reporting.

3. Explore practical examples for implementing CCM for IT Controls.

Diligent

Agenda

1. Introduction to Continuous Control Monitoring for IT
2. Key Principles and Components of CCM for IT Controls
3. Before You Get Started
4. Benefits of CCM for IT Controls
5. Assessing Readiness of CCM for IT Controls
6. Getting Started

Introduction to Continuous Control Monitoring for IT

Diligent

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

Definition of CCM

Diligent

A look back to 2023

Major Cybersecurity Incidents

Putting it in perspective…

In 2023, there were **2,814** publicly disclosed data breach incidents accounting for **8,214,886,660** breached records.

IT Governance Blog Release, February 5, 2024

Key trends influencing the threat environment…

1. AI
2. Sophisticated ransomware operators
3. Data breaches
4. Geopolitical tensions
5. IoT and OT

Royal Mail

In January 2023, UK's postal service was hit by a ransomware attack that resulted in halted deliveries, large revenue losses, and £10m on ransomware remediation.

T··Mobile·

International telecoms giant admitted that 37 million customers had their personal data accessed via an API attack.

USA.gov

Microsoft discovered a Chinese cyber-espionage campaign that enabled access to customer emails including US State and Commerce Departments and other US agencies.

23andMe

The DNA testing firm confirmed that threat actors claimed possession of 20 million records of sensitive information, affecting over 6 million individuals.

MGM RESORTS INTERNATIONAL™

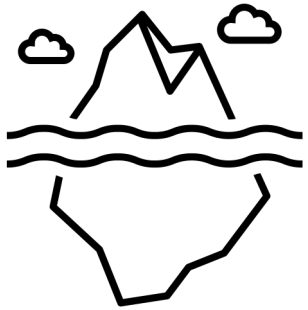
In September 2023, hotels and casinos giant experienced a ransomware attack affecting critical parts of its business for several hours resulting in more than $100m in damages.

Infosecurity Magazine Release, December 12, 2023

Why is CCM Important?

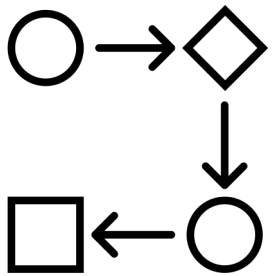
Complexity

In the modern business landscape, organizations face increasing complexity and risk.



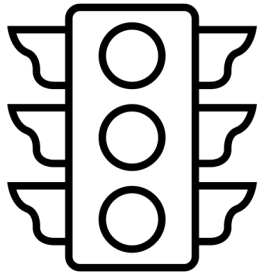
Efficiency

Streamlines IT control monitoring by automating routine tasks and providing insights into control effectiveness



Compliance

Helps ensure continuous compliance with regulations and frameworks by providing ongoing assurance that controls are functioning effectively



Diligent

Automated IT Control Testing Example

A Fortune 100 Company

General Requirements

- Automated way to ingest and analyze large amounts of data for the purposes of verifying IT controls

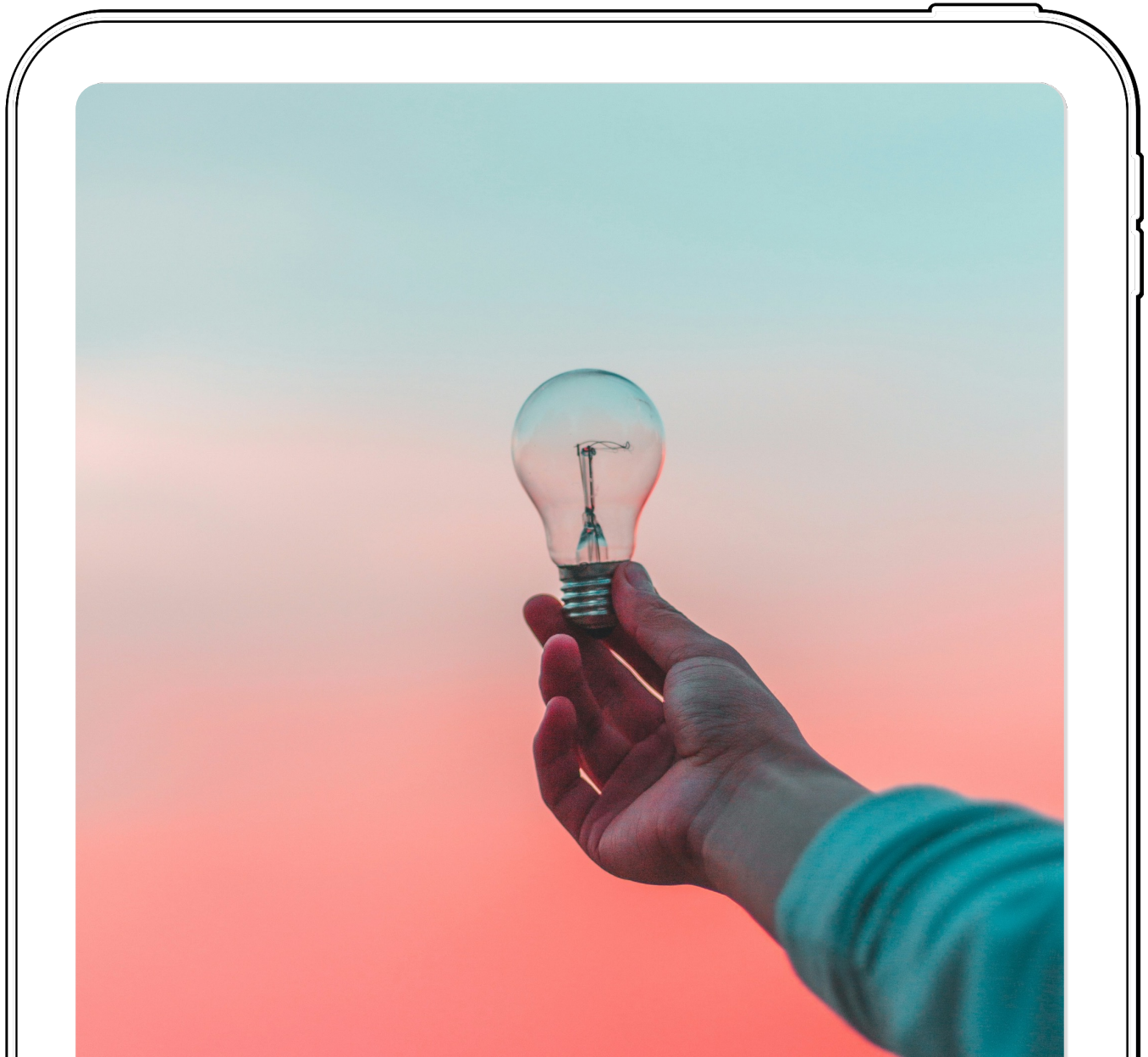
Lessons Learned

- Sampling is absolutely NOT enough, especially in IT
- Never be able to catch up if you stay looking backwards
- Proactive monitoring potentially keeps potential damage under control

Diligent

Significance of CCM

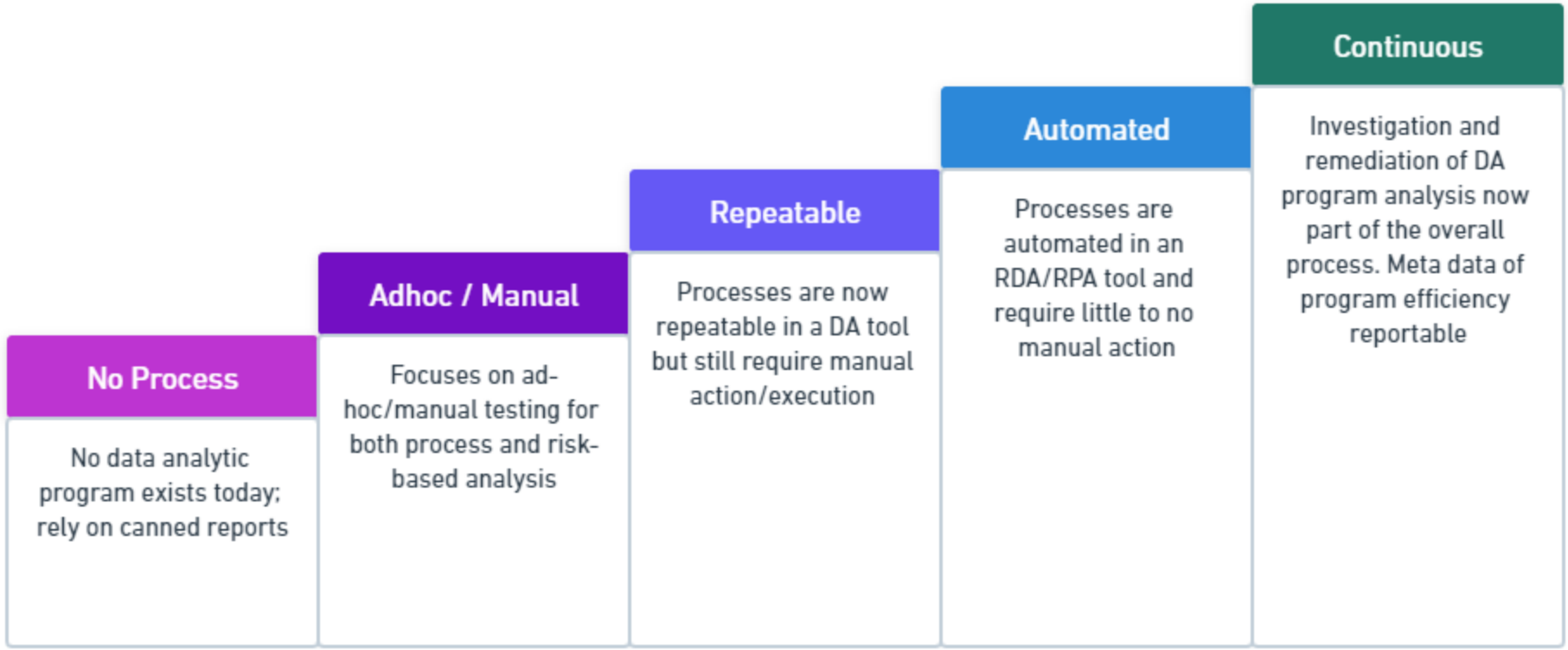
- **Timely Risk Identification**
  - Rapid detection of IT control weaknesses and vulnerabilities.
  - Allows for immediate corrective action.
- **Cost-Efficiency**
  - Reduces the cost of manual IT audits and compliance checks.
  - Maximizes resource allocation.
- **Enhanced Compliance**
  - Ensures adherence to regulatory and/or best practice requirements.
  - Reduces the risk of fines and penalties.

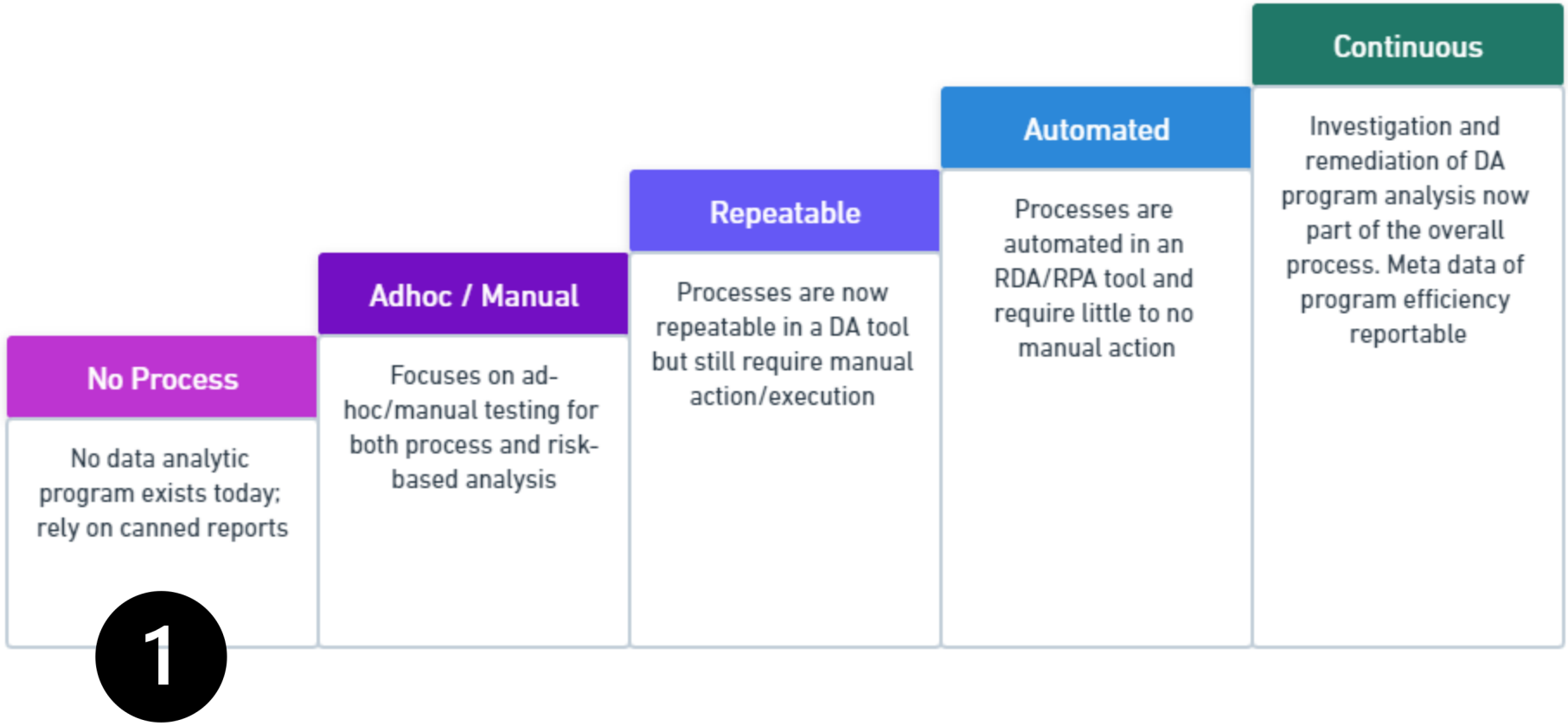


Diligent

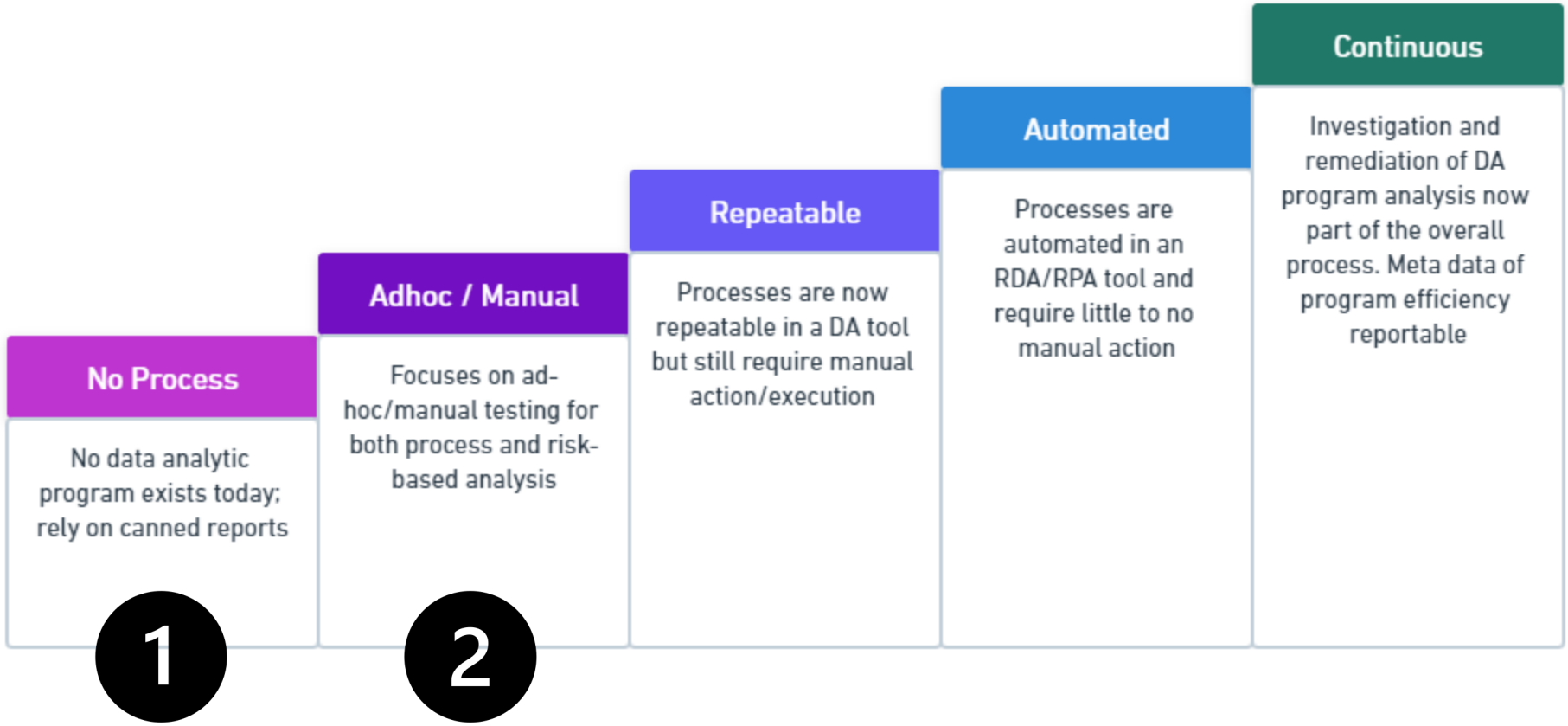
Key Principles and Components of CCM for IT Controls

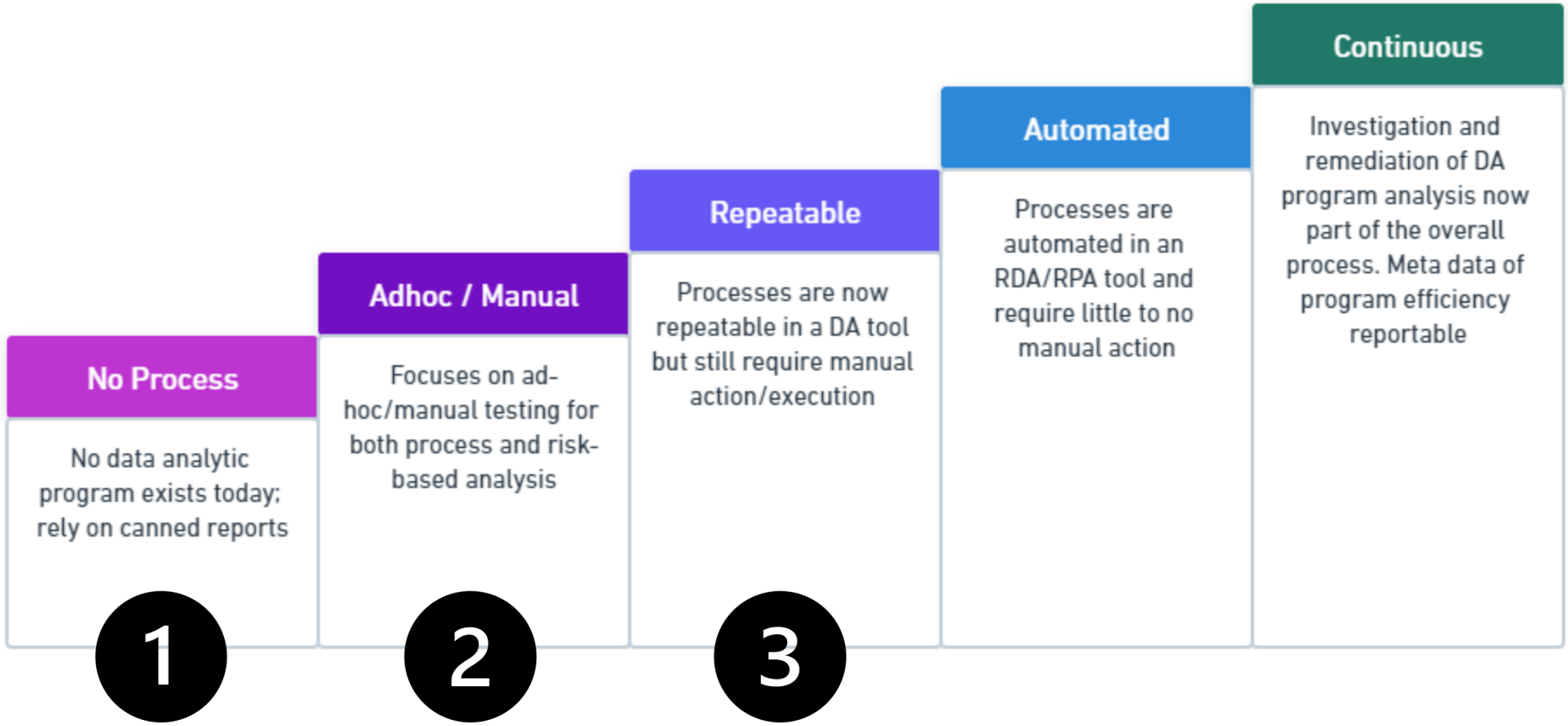
Diligent



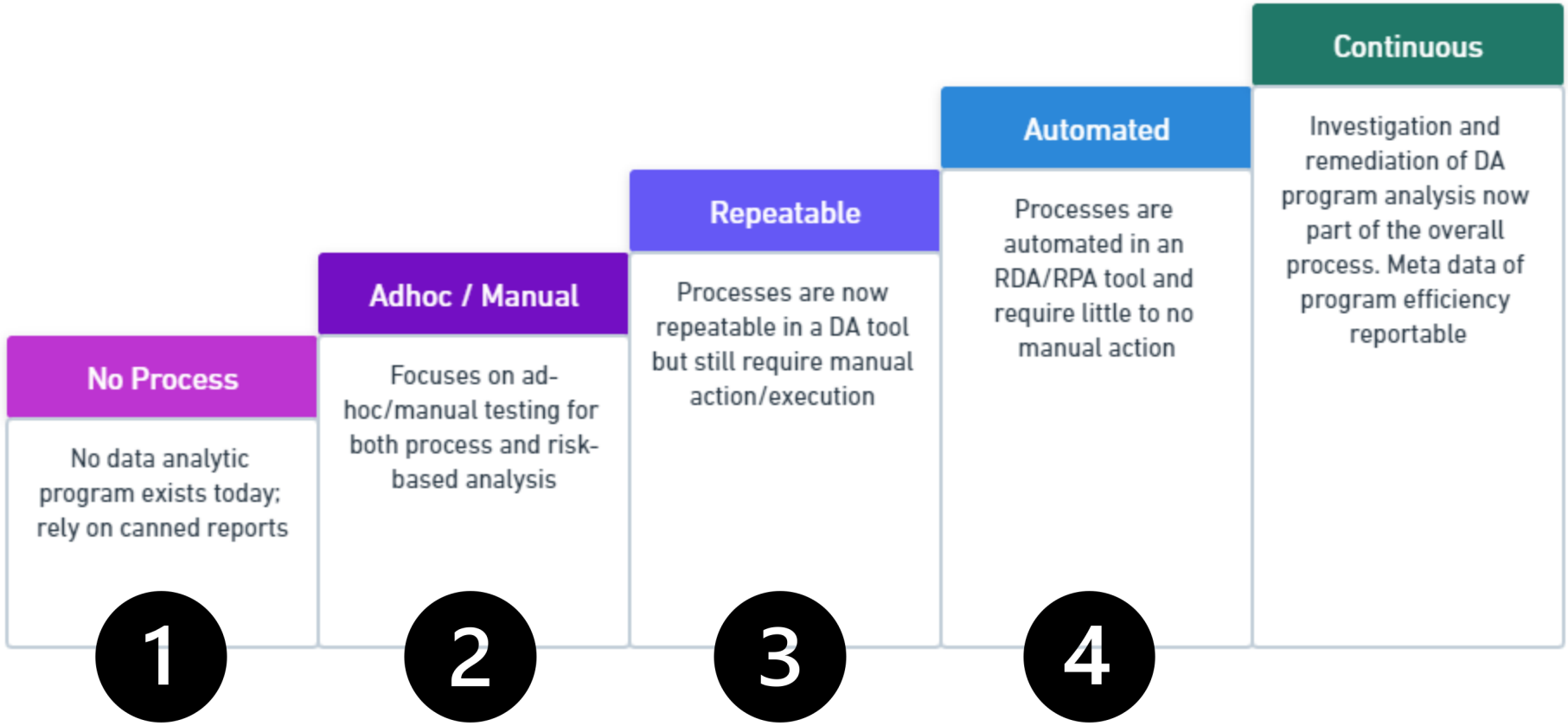


Diligent

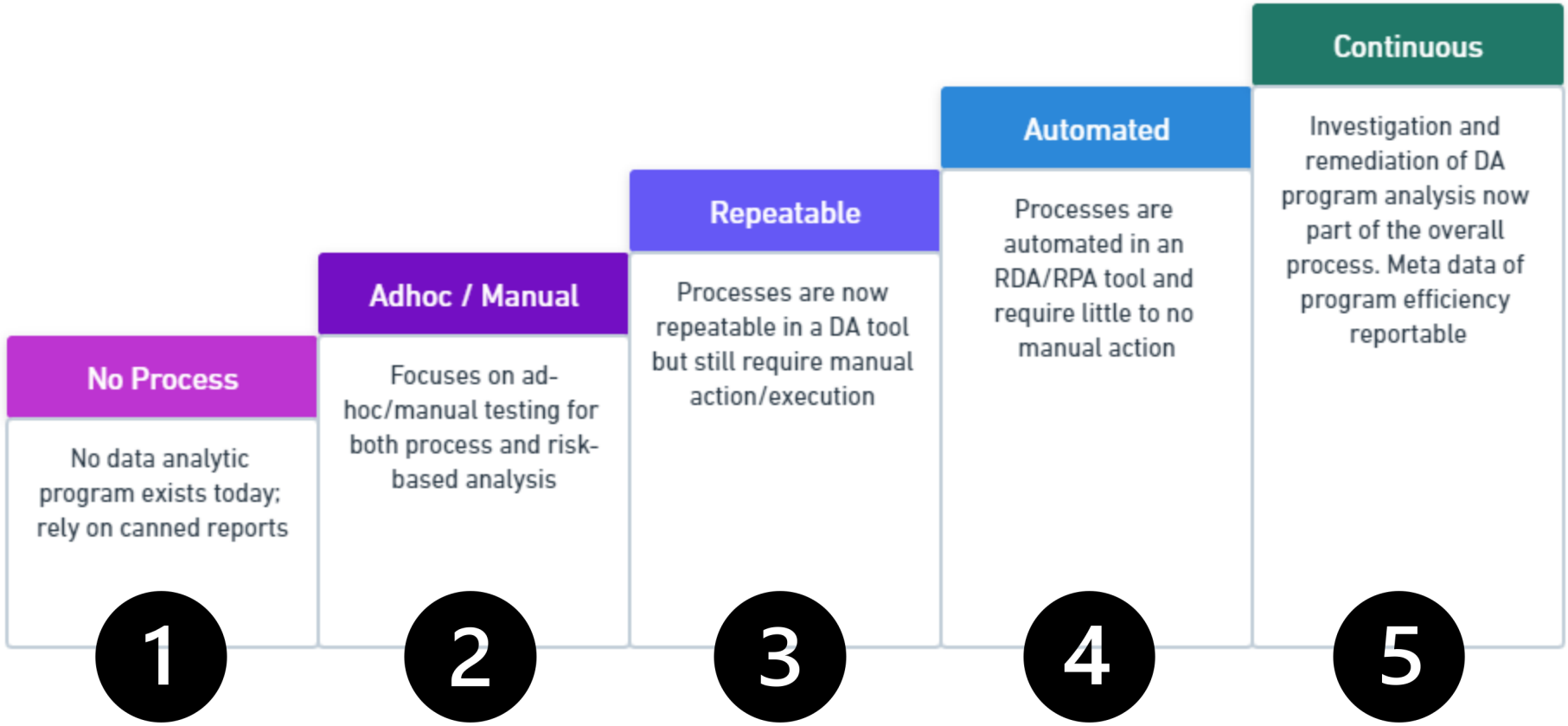




Diligent



Diligent

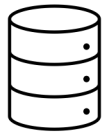


Diligent

Key Components

Automated Data Collection

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



Rule Engine

- Define specific rules and thresholds that indicate IT 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.

Diligent

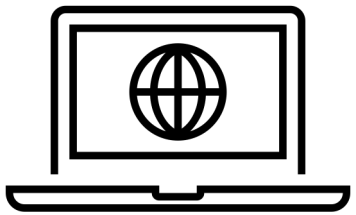
Before You Get Started

Diligent

Key Areas to Begin With

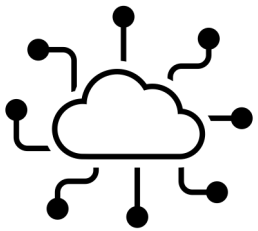
User Account Management

- Obsolete User Access
- User Account Information Discrepancies
- Delays in User Account Deactivation
- Dormant Accounts



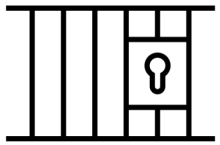
System Access Management

- Terminated Employees with Active Application Access
- Suspicious Login Activity (different country / off hours)
- Non-IT / System Owner Users with Admin Access
- Service Account Used On Multiple Systems



Vulnerability Management

- Compare vulnerability scans with the Common Vulnerabilities and Exposure (CVE)
- Compare subsequent vulnerabilities scans to identify recurring vulnerabilities
- Determine the mean time to remediate a vulnerability
- Report on potential at-risk hosts by determining percentage of vulnerabilities are linked to a host.



Diligent

Benefits of CCM for IT Controls

Diligent

"Continuous auditing could save 40% to 60% of the time wasted in audits waiting for auditees to prepare data, verify data accuracy, preparing reports, getting responses, etc."

Abdulrahman Sobhi, Head of Group Digital Audit Unit

Gulf Insurance Group

Diligent

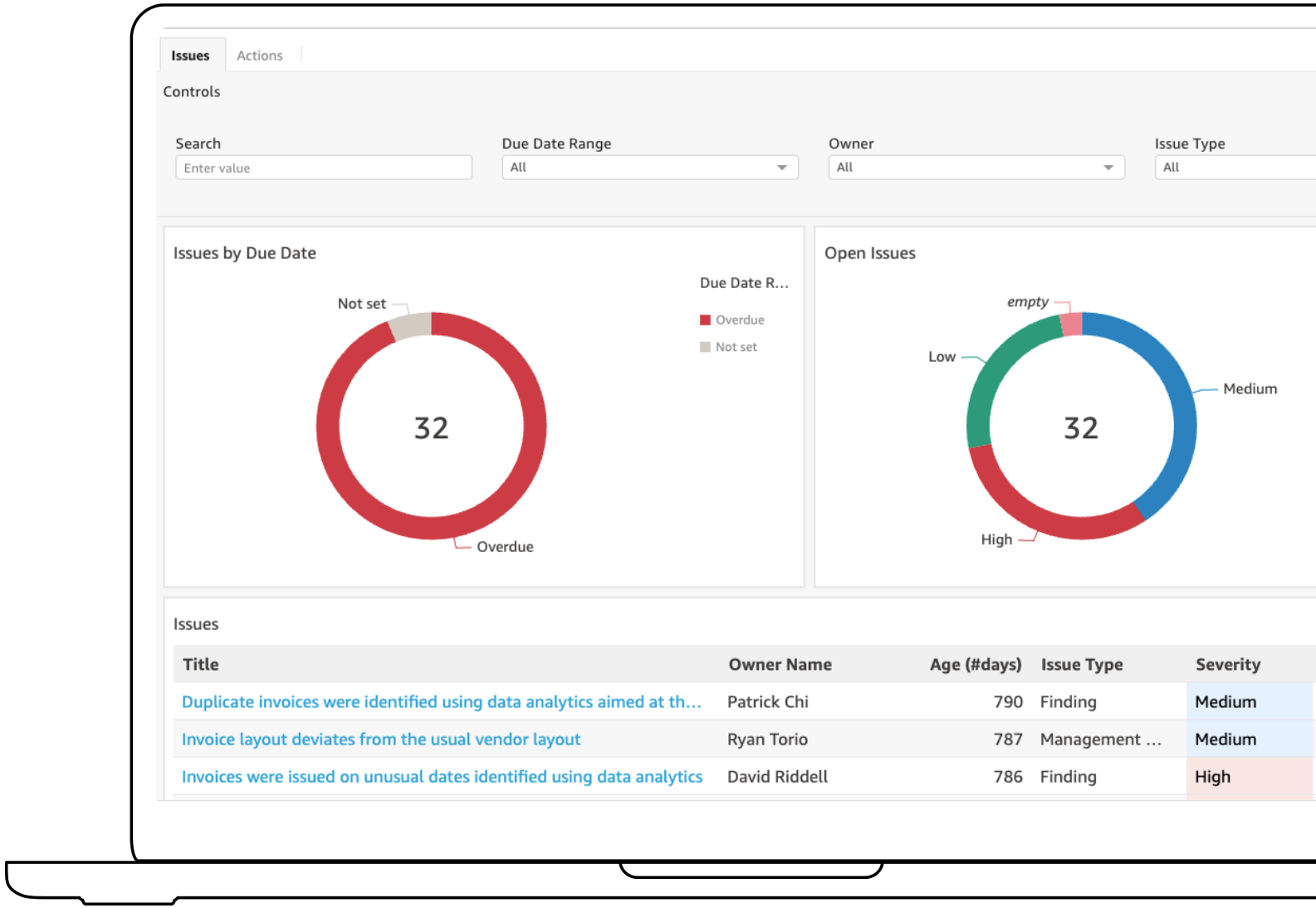
Real-Time Reporting

- **Instant Insights**
  - Provides immediate insights to decision-makers.
  - Enables proactive decision-making.
- **Data-Driven Decisions**
  - Equips leaders with the information needed for strategic planning.
  - Supports data-driven decision-making.

Diligent

Exposure to Senior Leadership

- **Visuals Instead of Detail Data**
  - Clues if SLA were met
  - Highlight Corporate Level Risks
- **Everything Should Be Actionable**
  - Clear Indicators of Focus Areas
  - Still Provide Mechanism for Deeper Dive



Diligent

Increased Accountability

- **Transparent Reporting**
  - Demonstrates accountability to stakeholders.
  - Builds trust and confidence.
- **Ethical Conduct**
  - Upholds ethical standards by identifying and addressing control breaches.

Diligent

Regulatory Compliance

- **Adherence to Regulations**
  - Ensures compliance with industry-specific regulations or frameworks such as ISO 27000, NIST, Center for Internet Security (CIS), HITRUST Common Security Framework (CSF) etc.
  - Provides documented evidence for audits.
- **Audit Trail**
  - Maintains a detailed audit trail of control activities.
  - Facilitates regulatory reporting.

Diligent

Assessing Readiness of CCM for IT Controls

Diligent

Assessing Organizational Readiness

Leadership Commitment

- Top-Down Support
- Must get buy-in from leadership
- Set the tone for a culture of compliance

Technological Infrastructure

- Evaluate capacity of Existing Technology
  - Data availability
- Identify gaps in technology

Data Quality

- Ensure the integrity, accuracy and completeness of data
- Data cleansing and validation

Employee Expertise

- Assess the proficiency of the audit and IT teams
- Identify gaps in skills
- Provide training on CCM tools and processes

Assessing Organizational Readiness

Example

- Top-Down support saves time in requesting corporate resource allocation
- Awareness throughout, share across organization
- Involve others, particularly business owners

Diligent

Challenges and Mitigations

Common Challenges

- Resistance to change
- Resource constraints
- Data privacy concerns.

Solutions

- Change management initiatives
- Resource allocation strategies
- Data encryption
- Compliance with data privacy regulations.

Diligent

Getting Started

Diligent

Implementing CCM

Tactical Approach

Processes / Controls

1. Identify IT processes or controls

- Through assessments define scope of control assurance.
- Determine priority IT controls for continuous monitoring.

Control Objectives

2. Identify IT control objectives (or goals) and key assurance assertions for each control objective.

Automated Tests

3. Define automated tests (or metrics) that will drive success or failure criteria of each assertion

Frequency

4. Determine the schedule / frequency, ensuring to test at a point in time close to when the transactions or processes occur.

Communicate

5. Implement processes for managing alerts, including communicating, investigating, and remediating any exceptions / control weaknesses.

Continuous Improvement

Diligent

Diligent

Questions?

Alex Fung

LinkedIn: https://www.linkedin.com/in/alex-fung-a2281422/

Chris Trepte

LinkedIn: https://www.linkedin.com/in/chris-trepte-60b02662/


Diligent