Designing an Agile, Just-in-Time approach to Ethics and Compliance Risk Assessments
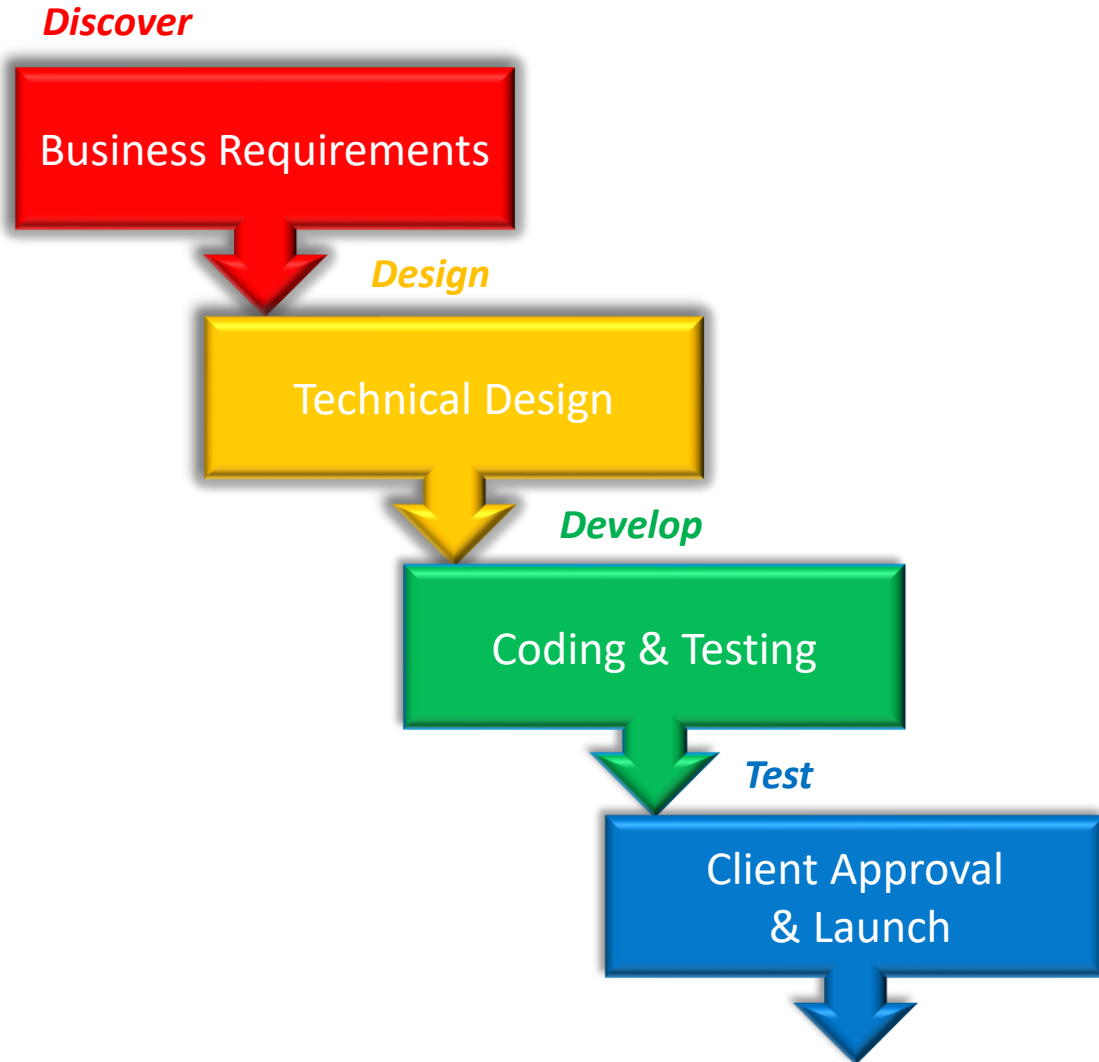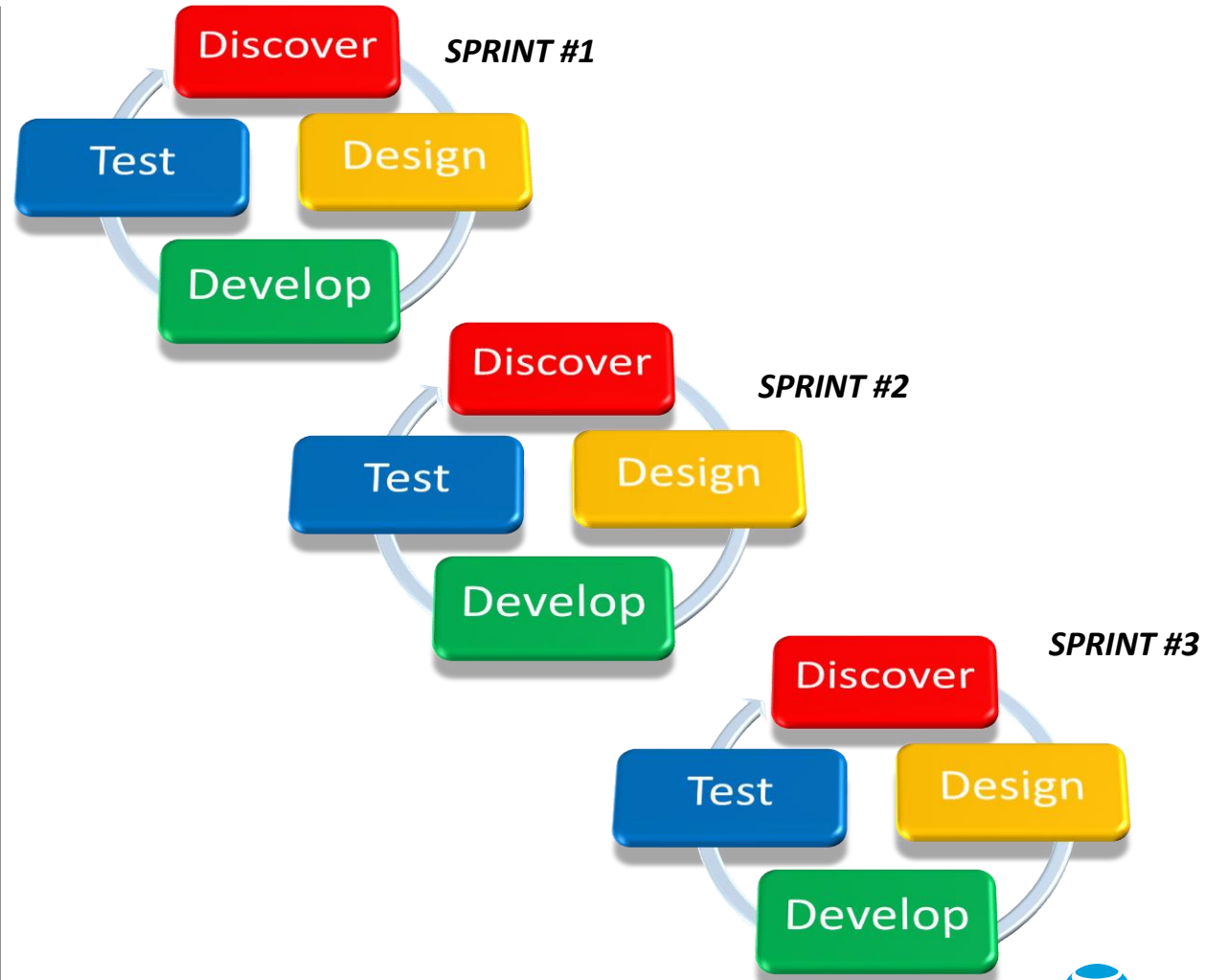
June 2022

AT&T

Agenda

- What does Agile mean?

- The Golden Thread/AT&T's Chief Compliance Office Risk Assessment Cycle

- Enabling the Business – Giving Time Back

- Ad-Hoc Risk Assessment Process

- Inspire Intentional Integrity – Business Ownership of Risk

Waterfall vs. Agile

Discover

Business Requirements

Design

Technical Design

Develop

Coding & Testing

Test

Client Approval & Launch

The **Waterfall** development method is a linear and sequential approach

Discover — SPRINT #1
Test
Design
Develop

Discover — SPRINT #2
Test
Design
Develop

Discover — SPRINT #3
Test
Design
Develop

The **Agile** development method is based on iterative and incremental development.
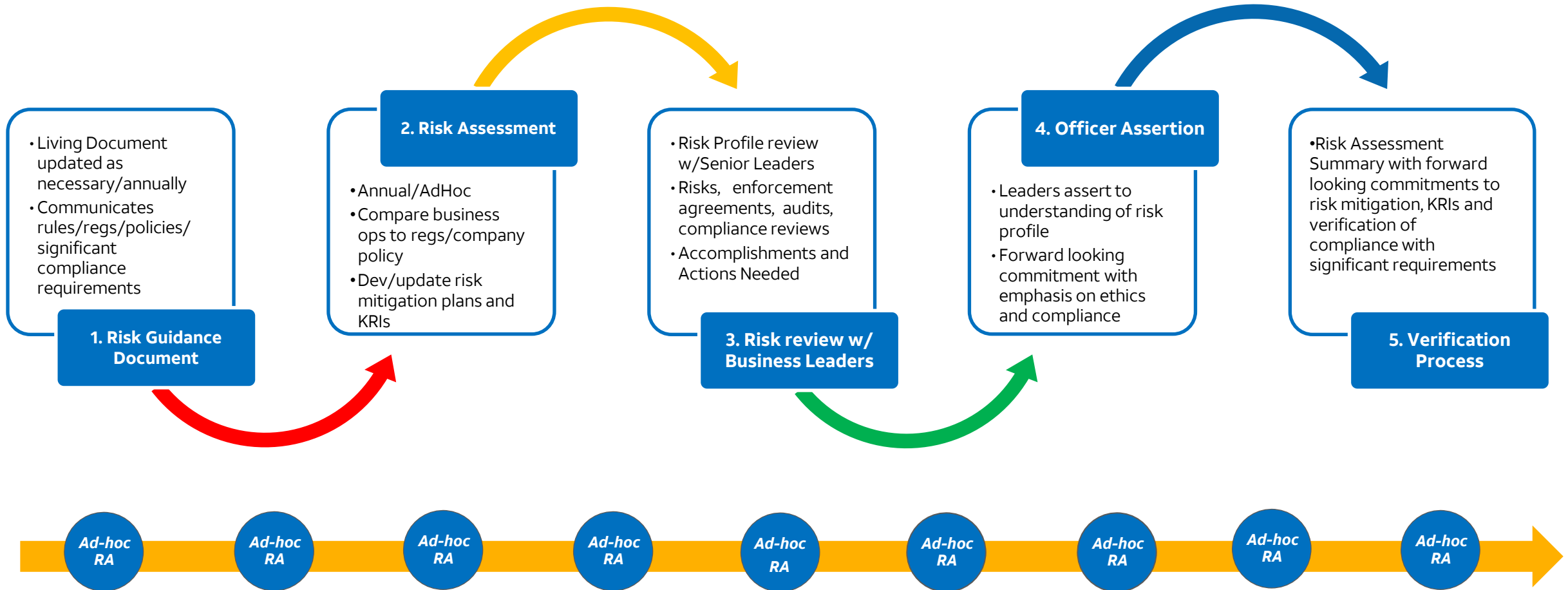
The Principles of the Agile Manifesto

- Example of Agile setup with Compliance Technology team

- Deliver MVP as soon as possible and keep improving it

- Can Agile methodology be applied to compliance?

1 **SATISFY THE CUSTOMER** through early and continuous delivery of valuable software.

2 Welcome **CHANGING REQUIREMENTS**, even late in development. Agile processes harness change for the customer's competitive advantage.

3 **DELIVER WORKING SOFTWARE FREQUENTLY**, from a couple of weeks to a couple of months, with a preference to the shorter timescale.

4 Business people and developers must **WORK TOGETHER DAILY** throughout the project.

5 Build projects around **MOTIVATED INDIVIDUALS**. Give them the environment and support they need and trust them to get the job done.

6 The most efficient and effective method of conveying information to and within a development team is **FACE-TO-FACE CONVERSATION**.

7 **WORKING SOFTWARE** is the primary measure of progress.

8 Agile processes promote **SUSTAINABLE DEVELOPMENT**. We should be able to maintain a constant pace indefinitely.

9 Continuous attention to **TECHNICAL EXCELLENCE AND GOOD DESIGN** enhances agility.

10 **SIMPLICITY** – the art of maximizing the amount of work not done – is essential

11 The best architectures, requirements, and designs emerge from **SELF-ORGANIZING TEAMS**

12 At regular intervals, **THE TEAM REFLECTS** on how to become more effective, then tunes and adjusts its behavior accordingly.
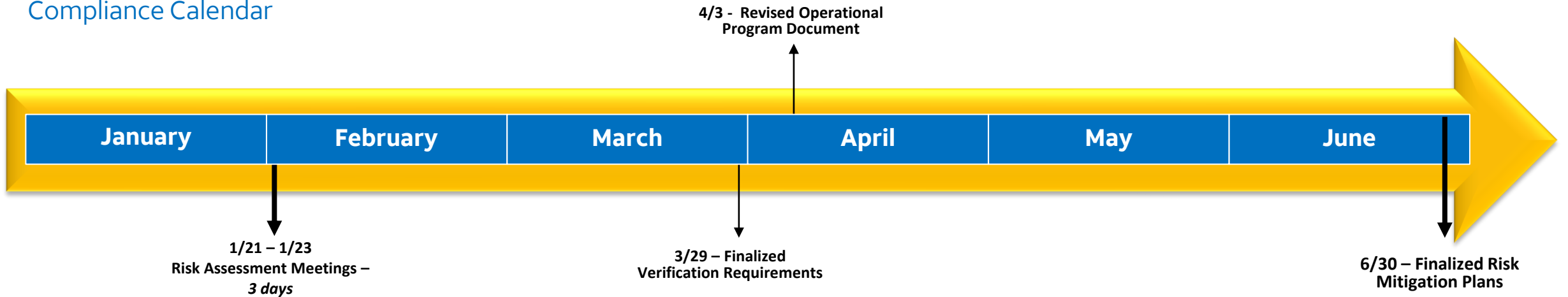
The Golden Thread/AT&T's Compliance Cycle

- Living Document updated as necessary/annually
- Communicates rules/regs/policies/ significant compliance requirements

1. Risk Guidance Document

2. Risk Assessment

- Annual/AdHoc
- Compare business ops to regs/company policy
- Dev/update risk mitigation plans and KRIs

- Risk Profile review w/Senior Leaders
- Risks, enforcement agreements, audits, compliance reviews
- Accomplishments and Actions Needed

3. Risk review w/ Business Leaders

4. Officer Assertion

- Leaders assert to understanding of risk profile
- Forward looking commitment with emphasis on ethics and compliance

- Risk Assessment Summary with forward looking commitments to risk mitigation, KRIs and verification of compliance with significant requirements

5. Verification Process

Ad-hoc RA   *Ad-hoc RA*   *Ad-hoc RA*   *Ad-hoc RA*   *Ad-hoc RA*   *Ad-hoc RA*   *Ad-hoc RA*   *Ad-hoc RA*   *Ad-hoc RA*

AD-HOC RISK ASSESSMENT = ON DEMAND, DYNAMIC, MINI-RISK ASSESSMENTS

5

Enabling the Business – *Giving time back*

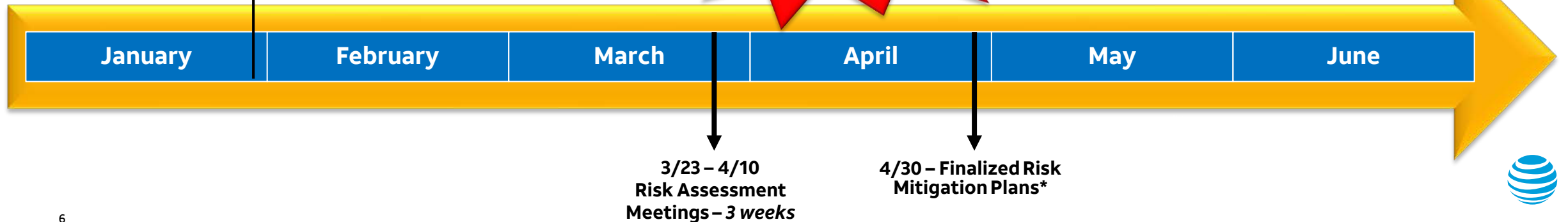**Pre-Evolution (aligned with Waterfall Processes)**

Compliance Calendar

4/3 - Revised Operational Program Document

January	February	March	April	May	June

1/21 – 1/23
Risk Assessment Meetings –
3 days

3/29 – Finalized Verification Requirements

6/30 – Finalized Risk Mitigation Plans

1/31 - Revised Risk Guidance Document

74% reduction in RA cycle time YoY

Post-Evolution (Agile)
Compliance Calendar

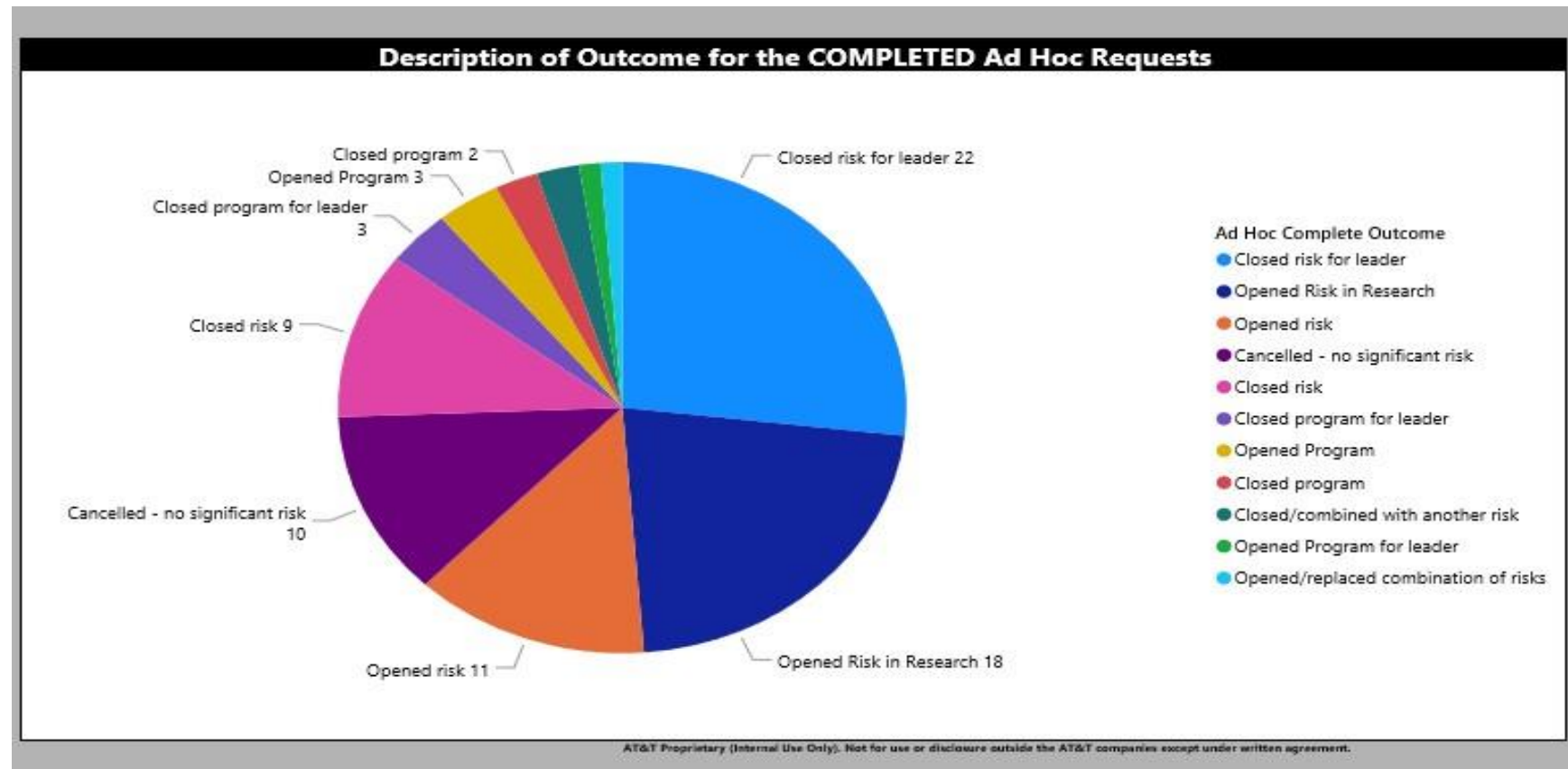| January	February	March	April	May	June

3/23 – 4/10
Risk Assessment Meetings – *3 weeks*

4/30 – Finalized Risk Mitigation Plans*

6

Enabling the Business – *Giving time back*

Ad-hoc RA → Ad-hoc RA → Ad-hoc RA → Ad-hoc RA → Ad-hoc RA → Ad-hoc RA → Ad-hoc RA → Ad-hoc RA → Ad-hoc RA

Enhancements Introduced:

- Formalized *Risk-In-Research*
- Treatment at a leader level
- Lasting record

Description of Outcome for the COMPLETED Ad Hoc Requests

- Closed risk for leader 22
- Closed program 2
- Opened Program 3
- Closed program for leader 3
- Closed risk 9
- Cancelled - no significant risk 10
- Opened risk 11
- Opened Risk in Research 18

Ad Hoc Complete Outcome
- Closed risk for leader
- Opened Risk in Research
- Opened risk
- Cancelled - no significant risk
- Closed risk
- Closed program for leader
- Opened Program
- Closed program
- Closed/combined with another risk
- Opened Program for leader
- Opened/replaced combination of risks

Inspire Intentional Integrity – Business Ownership

Business Unit Leader "Risk Profile"

AT&T Communications Risk Profile – AT&T Business
As of Month, Year*

Table of Contents

1. Summary
2. Compliance Programs
3. Open Risks
4. Mitigated and Closed Risks
5. Risks In Research
6. Enforcement Agreements & Merger Conditions
7. Compliance Reviews
8. Enabling the Business

*This deck represents the current status of risk related activity for the AT&T Communications Company as identified by the Chief Compliance Office (CCO). It is a snapshot in time as well as a reflection of the compliance related activity that took place during the 2021-2022 risk assessment cycle.

Officer Assertion

- **Big picture sample statement**

  - *I am aware that there are certain risks to AT&T as a result of the work performed by my organization and the information my organization accesses or manages.*

- **Supported by the Risk Profile -** Signature AFTER CCO Leadership engagement. CCO able to attest to first-hand knowledge of Leadership coverage. **Sample language**

  - *I understand the risk profile presented to me and I support the mitigation plans necessary to address these compliance matters.*

8