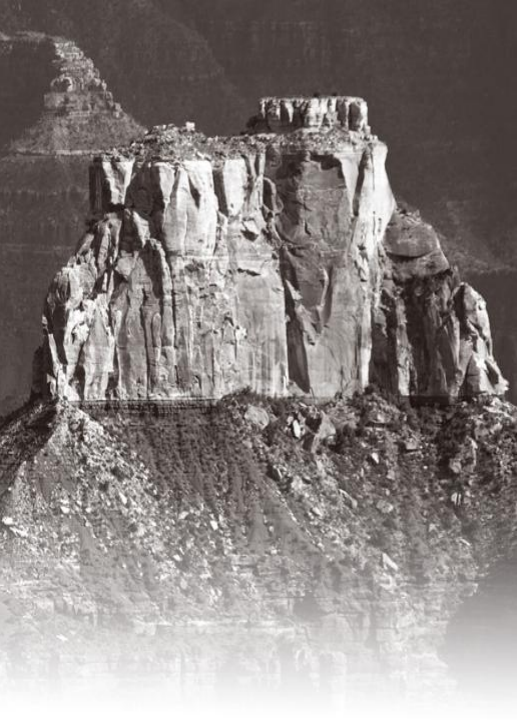


The Journey towards Operationalizing Third Party Risk Management

RSA GRC Summit 2014

Paul Kriebel, Deloitte & Touche LLP
Christian Caspersen, SunTrust Banks Inc.

2014 RSA Archer grc summit

#ArcherSummit

EMC²

RSA

About the Presenters

Paul Kriebel

Manager

Cyber Risk Services

Deloitte & Touche, LLP

Paul is a Manager with Deloitte's Cyber Risk Services practice and has more than 20 years of experience, providing services to clients related to enterprise risk management, technology risk management, information security, and related implementations services.

Paul has worked for multiple fortune 100 organizations focused on developing their enterprise risk management and GRC technology programs. Paul is one of the Deloitte contacts for the RSA Archer Alliance and also is a member of the Deloitte GRC technology services practice.

Paul is the Project Manager for the RSA Archer GRC tool implementation at SunTrust for the TPRM engagement.

Christian Caspersen

Senior Vice President

Corporate Operational Risk Management

SunTrust Bank, Inc.

Chris is the implementation Lead for the RSA Archer GRC tool, which allows SunTrust to best manage the Third Party Risk Management program. The development consists of a comprehensive risk assessment, on-going monitoring routines, and issues management.

Chris is responsible for measuring and monitoring the effectiveness of the Corporate Operational Risk management program within the Consumer line of business and Vendor Management function. Advise and coordinate on their operational risk management activities. Specific activities include: effectively implementing the risk assessment of internal processes, QA and QC testing activities, issues management, and ongoing management reporting.

Preface

Traditional approaches to operationalizing risk management in the financial services industry are changing in response to regulatory expectations. Regulatory scrutiny has accelerated the requirement for banks to manage third party risk in the context of operational risk. This new intersection between Compliance Management and Operational Risk Management requires financial institutions to understand the risks specific to the products/ services the organization wants to source to a third party and then determine how these risks may be amplified based on the nature, scope and scale of the third party relationship.

To this end, SunTrust has engaged Deloitte to support with operationalizing SunTrust's third party risk management program as the organization leverages its sourcing strategy to expand its product/ service offering and presence in the marketplace.

Introduction

- The SunTrust has implemented Version 1.0 of its RSA Archer solution for Third Party Risk Management (TPRM). However, the journey towards implementing operational risk management capabilities from TPRM at SunTrust is underway.
- SunTrust has engaged Deloitte to help with the implementation of the evolving TPRM program processes in RSA Archer.
- Several other RSA Archer implementation initiatives are also underway and in various states of maturity.
- Coordinating the SunTrust RSA Archer implementation requires Governance and common taxonomies across the enterprise if the individual initiatives are to succeed on a shared platform.

Goal

To implement regulatory requirements related to third party risk management (TPRM) in an ever-changing internal environment towards the goal of a common operational risk management capability that can be leveraged across the enterprise.

Executive Summary

Driven by regulatory requirements and internal needs, SunTrust is moving to develop an enterprise-wide operational risk management capability.

Plan

- Launch initiative to redesign their TPRM processes to meet regulatory requirements.
- Launch initiative to automate those processes in RSA Archer.

Reality

- Automation of manual processes alone is not a panacea.
- Need to meet the intent of the regulatory requirement – i.e., managing relationships.
- Multiple stakeholders with different/redundant processes on a single platform.

Solution

- Understand– the benefits of automation: transparency, standardization, etc.
- Vision – see the long term implications of short term decisions.
- Operationalize – implement a long-term solution that is architected for making risk management an operational risk management activity.

The Plan

#ArcherSummit

Implementation Objectives

Technology Objectives

- To define a strategic technology roadmap for the automation of the TPRM program and processes over time through iterative development
- To develop a centralized platform to enable the execution of TPRM activities that is scalable and extensible to address future program and regulatory considerations
- To implement the solution in a phased manner to achieve incremental successes and long-term improvement as the TPRM program matures

Benefits

- ***Automation*** of the TPRM lifecycle on the RSA Archer technology platform, including workflows, reporting, and ongoing monitoring
- ***Standardization*** of the TPRM processes to provide consistency and integrity across the enterprise
- ***Transparency*** to provide an enterprise-wide view of third party/risk profiles and to demonstrate TPRM program effectiveness to relevant internal and external stakeholders

The Challenge

#ArcherSummit

Proactively Responding

In 4Q 2013, both the OCC and FRB released enhanced guidance for the risk management of third-party relationships

Office of Comptroller of the Currency (OCC)

In OCC Bulletin 2013-29, the Office of the Comptroller of Currency clearly states: "A bank's use of third parties ***does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws***".

Consumer Financial Protection Bureau (CFPB)

In CFPB Bulletin 2012-03, issued April 13, 2012, the CFPB obviously concurs: The CFPB ***"expects supervised banks…to oversee their business relationships with service providers in a manner that ensures compliance with Federal consumer financial law***".

United States Federal Reserve System

Guidance released on December 5, 2013 outlines the following important elements to a third party risk management program:

- Inherent risk assessment of the **service** being outsourced
- Due diligence and evaluation of the service provider
- Appropriate contract provisions and considerations **including third party incentives**
- Oversight and monitoring of services based on the contract provision and risks by teammates with ***"appropriate level of expertise and stature to manage the outsourcing arrangement"***
- Business continuity and contingency plans

"This guidance continues to confirm the ***necessity of the enhanced framework*** we have been defining and the regulatory expectation that risk management processes and controls be commensurate with the risk associated with the activity being performed by the service provider." Corporate Operational Risk Officer

Proactively Responding

In 4Q 2013, both the OCC and FRB released enhanced guidance for the risk management of third-party relationships

Office of Comptroller of the Currency (OCC)

In OCC Bulletin 2013-29, the Office of the Comptroller of Currency clearly states: "A bank's use of third parties ***does not diminish the responsibility of its board of directors and senior ma*** ***is perform*** ***complianc***

Consume

In CFPB B
CFPB obvi
supervise
relations
manner that ensures compliance with Federal consumer financial law".

United States Federal Reserve System

Guidance released on December 5, 2013 outlines the following important elements to a third party risk management program:

Inherent risk assessment of the **service** being

tions

the
th
re to

What does it mean?

*Banks need to focus on the **relationships** they have with Third Parties (and Fourth Parties)….*

"This guidance continues to confirm the ***necessity of the enhanced framework*** we have been defining and the regulatory expectation that risk management processes and controls be commensurate with the risk associated with the activity being performed by the service provider." Corporate Operational Risk Officer

Understanding the Guidance

Analogy – Buying your first car…

Scenario

- Teenage son wants to buy his first car for $25,000.
- Father makes $500K annually and could easily pay cash, but doesn't loan son money.
- So, the son applies to bank for a loan…
  - **Bank (to Son)**: Are you employed?
  - **Son**: Yes, at a McDougal's Hamburgers.
  - **Bank**: And you make…$5.25/hour?
  - **Son**: Yup.
  - **Bank**: OK….

Option A

- Bank loans to Son
- Son defaults…
- Bank goes after Son…
- *Doh*!

Option B

- Bank loans to Son (Father co-signs)
- Son defaults…
- Bank goes after Dad…
- Bank gets money back.

Conclusion

It is the Bank's <u>contractual</u> relationship with the Parent or Child that matters!

The Response

#ArcherSummit

TPRM Risk Assessment Process

Identification of third party risks enables improved contracting, monitoring and pro-active decision making.

Align Strategies to Goals + Determine Inherent Risk + Complete Due Diligence Assessments + Evaluate Residual Risk + Develop intelligent contracts +

Key Artifact Descriptions

Business Case - Outlines the business need and justification to commit resources towards a project

Inherent Risk Determination - Uncovers inherent risk and enables the risk/reward analysis that should be performed in order to protect the bank and clients

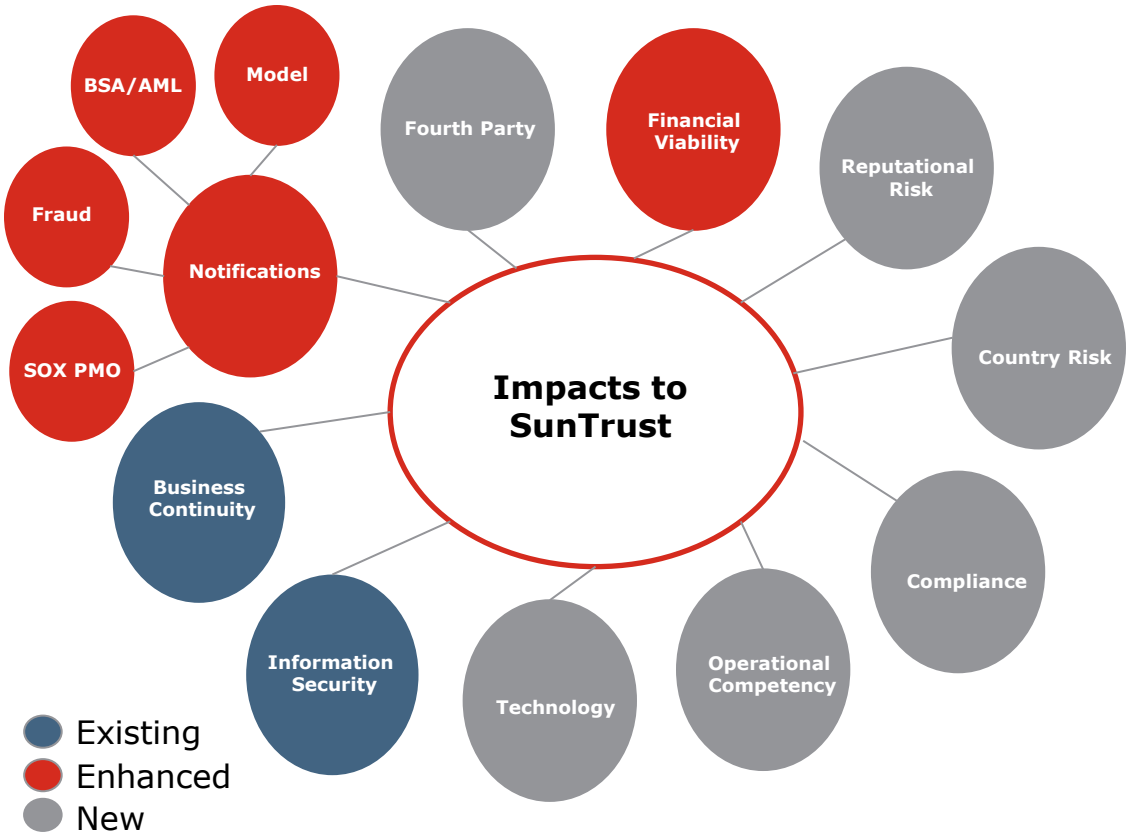
Due Diligence Assessments - Provides management with the risk assessment information needed to determine if a relationship would help achieve the business objectives and mitigate identified risks

Residual Risk Determination – After completing the general assessment of risks and alignment to the business strategy, management should review its ability to provide oversight and management of the proposed third party relationship on an ongoing basis.

Contracts – Ensures expectations of both third party and SunTrust are outlined in a written document prior to executing and entering the arrangement. Legal should review contracts prior to execution and should inhibit any subcontracting by the third party of its obligations to a fourth party until SunTrust performs its due diligence and is satisfied consistent standards will be met

Assessments and Notifications

The due diligence assessments identify potential impacts to SunTrust in the nine (9) areas of risk. The notifications provide awareness to the four (4) areas that further research of the service may be required per the notification areas standard processes.



Archer will *automatically identify* which due diligence assessments and/or notifications and will *trigger the need for an Assessment* to be completed for the potentially sourced product/service.

Strategic Roadmap

Deloitte recommended a strategic roadmap to establish a vision for the operationalization and automation of the TPRM program.

Establish and Automate an Overall Third Party Categorization and Risk Tiering Methodology

Establish and Automate Prioritized Third Party Risk Management Practices

Establish a formal data and RSA Archer governance model in alignment with enterprise standards

Establish, Automate and Coordinate select Third Party Risk Management Practices

Incremental TPRM Versions

Rather than a take "big bang" approach, Deloitte delivered foundational capabilities for TPRM Version 1.0, as the team develops incremental process and automation enhancements towards the vision of a Version 2.0. release.

	Proof of Concept	TPRM V1.0	TPRM V1.5
Objectives	• To **demonstrate** TPRM solution Proof of Concept (PoC) capabilities	• To **implement** existing TPRM processes	• To **enhance** process improvements towards Version 2.0
Key Activities	• Delivered Strategy and Roadmap for TPRM program • Demonstrated initial Assessments and Questionnaires to key stake holders and business owners • Built foundational TPRM capabilities	• Moved from ***Third Party-based approach to Service-based approach*** • Implemented existing TPRM processes • Delivered integrated solution for TPRM and Info Sec changes	• Implementing requested requirement enhancements, incremental process improvements ***towards industry-leading risk management capabilities***

Recent activities

Where we are headed

#ArcherSummit

TPRM Version 2.0 Objectives

The journey ahead includes developing an industry-leading operational risk management capability that can be leveraged across the enterprise and that can become a standardized model for operational risk management.

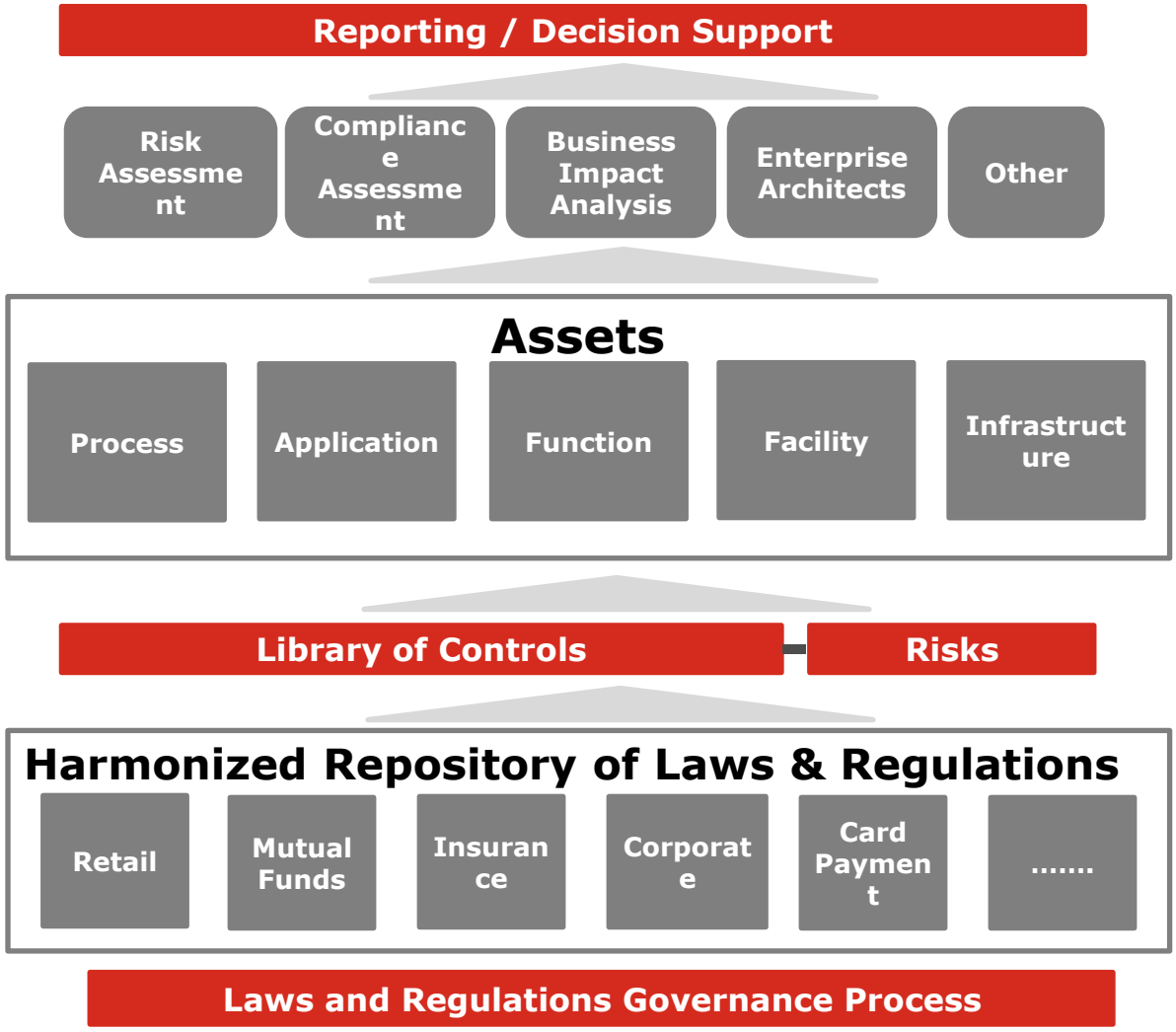
RSA Archer TPRM Version 2.0 Implementation

Objectives

- To establish a ***service baseline*** for TPRM based on service categories
- To establish a ***common approach*** to service and product risk management across the organization
- To ***reengineer processes*** in alignment with leading practices for TPRM
- To move towards an ***industry-leading Operational Risk Management capability***

Integrated Capability

Operationalizing asset, risk and compliance management capabilities



Enables **aggregated views** of risk and compliance

Various processes can utilize the **risk and control (linked to assets)** data as needed

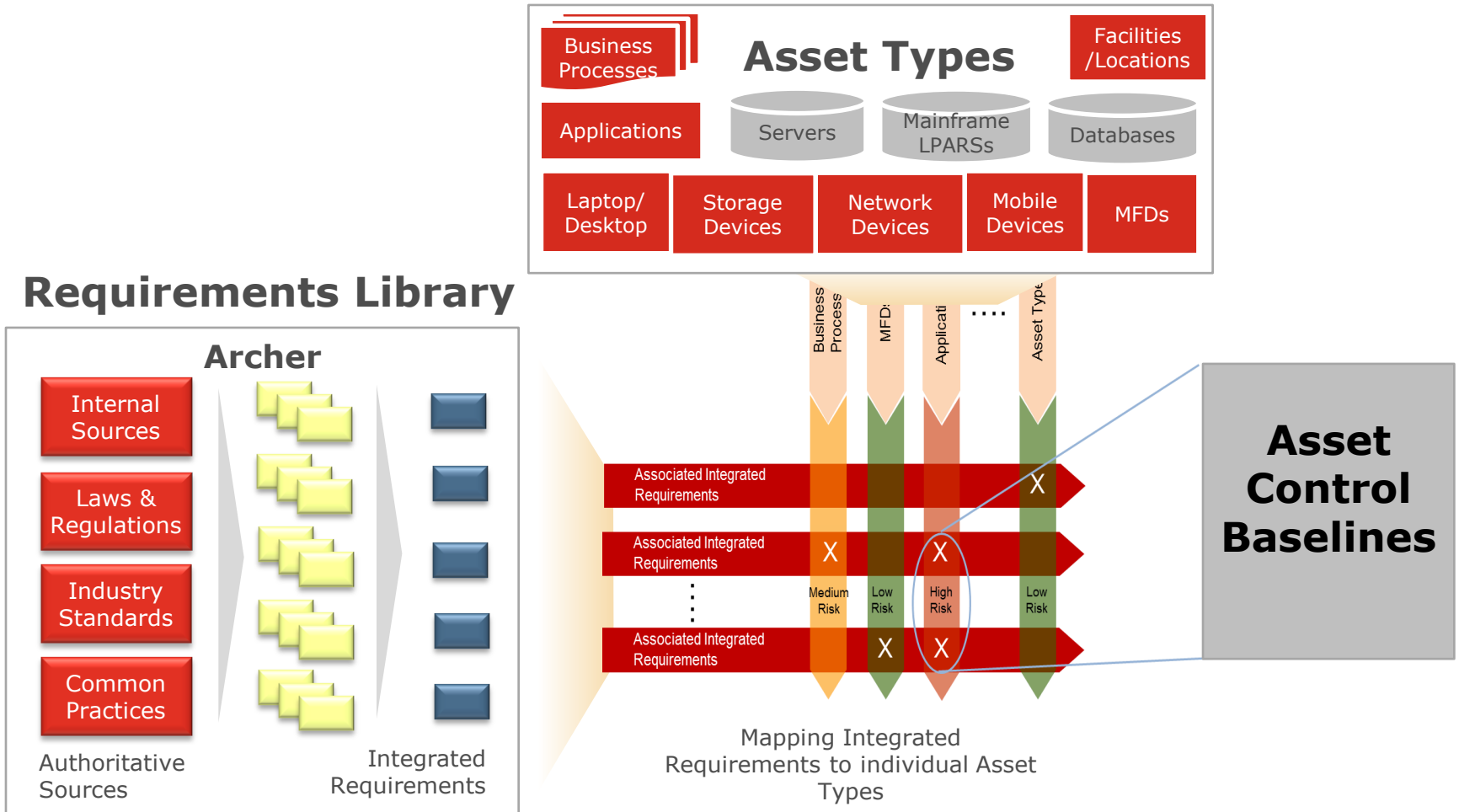
Asset inventory is a repository of enterprise processes, applications, infrastructure, functions and facilities. The asset inventory holds risk and control information, changing the existing process from compliance based to a **risk based model**

Risks and controls are linked to the repository of laws & regulations

Each division within the business has **visibility** into their specific requirements

Mapping the Environment

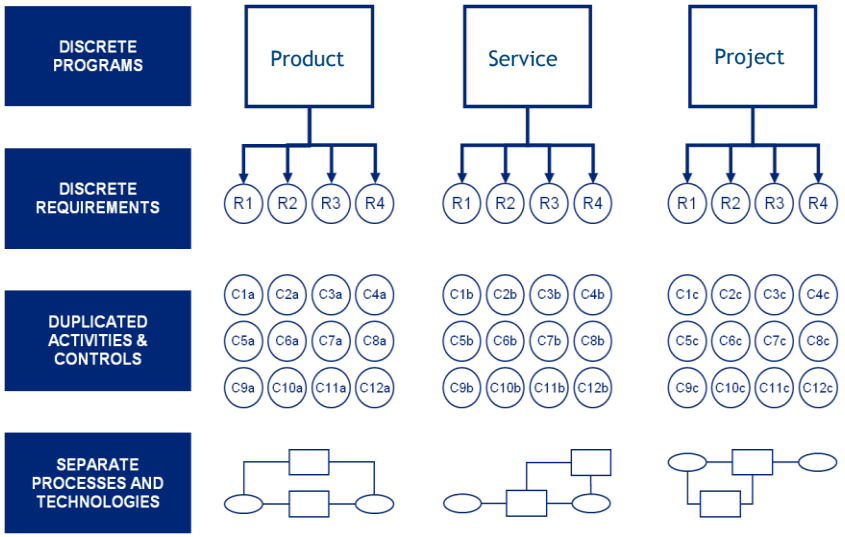
Defining a set of risk and control requirements for each asset type that is in-scope for ARM asset tracking and reporting.



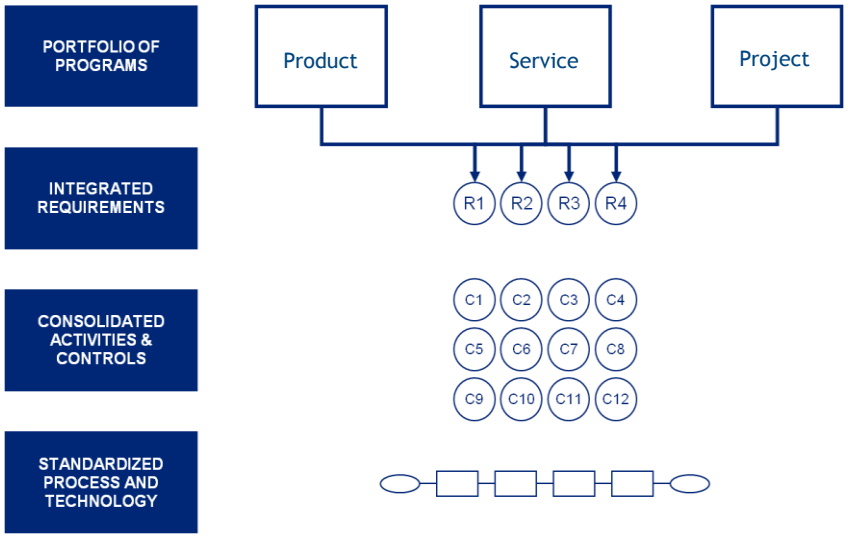
Future State

Establishing a harmonized operational risk management process will provide for consistent monitoring and reporting across the business.

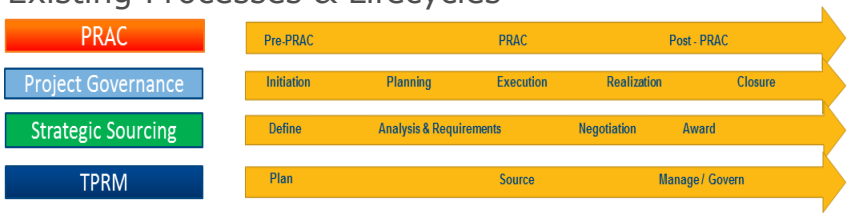
Inconsistency and **inefficiency** in managing requirements from ***multiple*** programs



Reduced cost and complexity with overlap removed and **common** requirements definition



Existing Processes & Lifecycles



Harmonized Process & Lifecycle

Thank you.

2014 RSA Archer grc summit

#ArcherSummit