GRC SUMMIT 2023

MIAMI, JUNE 14 & 15

Hosted by MetricStream

Autodesk GRC Journey

Clyde Tsai

Agenda

- Autodesk Overview
- Autodesk Trust Organization
- Autodesk Strategic Intent
- GRC Drivers @ Autodesk
- GRC Journey – Current State
- Business Value and Realized Benefits
- Priorities for Next Year
- Top Challenges (and Key Learnings)
- Additional Challenges (and Key Learnings)

Your Presenter Today

- Clyde Tsai
  - GRC Lead @ Autodesk
  - 15 years in GRC field
  - 10 years in Big 4 consulting

Autodesk Overview

Founded

1982

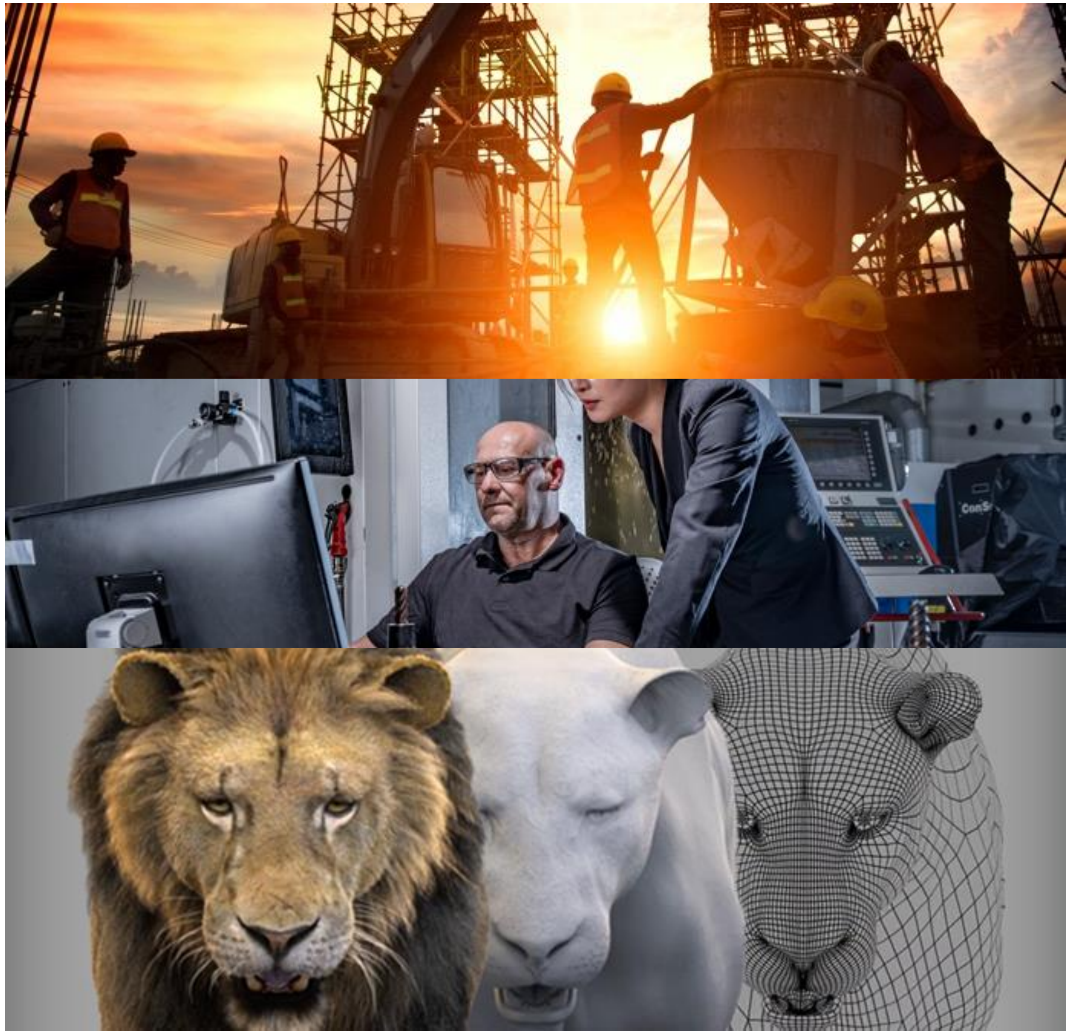
Headquarters

San Francisco, CA

Employees (2022)

13,400+ worldwide

$4.39B	6.04M	$1.1B
Total revenue	Total subscribers	R&D investment



Our industries

Architecture, Engineering, and Construction

Manufacturing

Media & Entertainment

Autodesk Strategic Intent

VISION | What inspires us?
A better world designed and made for all

MISSION | What do we do?
We empower innovators with design and make technology so they can achieve the new possible.

STRATEGY | How will we get there?
We deliver customers intuitive, powerful, and accessible technology that provides automation and insight for their design and make processes, enabling them to achieve better outcomes for their products, their businesses, and the world.

PRODUCTS
AutoCAD, Revit, Fusion 360, BIM Collaborate Pro, 3DS Max, Maya, Shotgrid, and many more

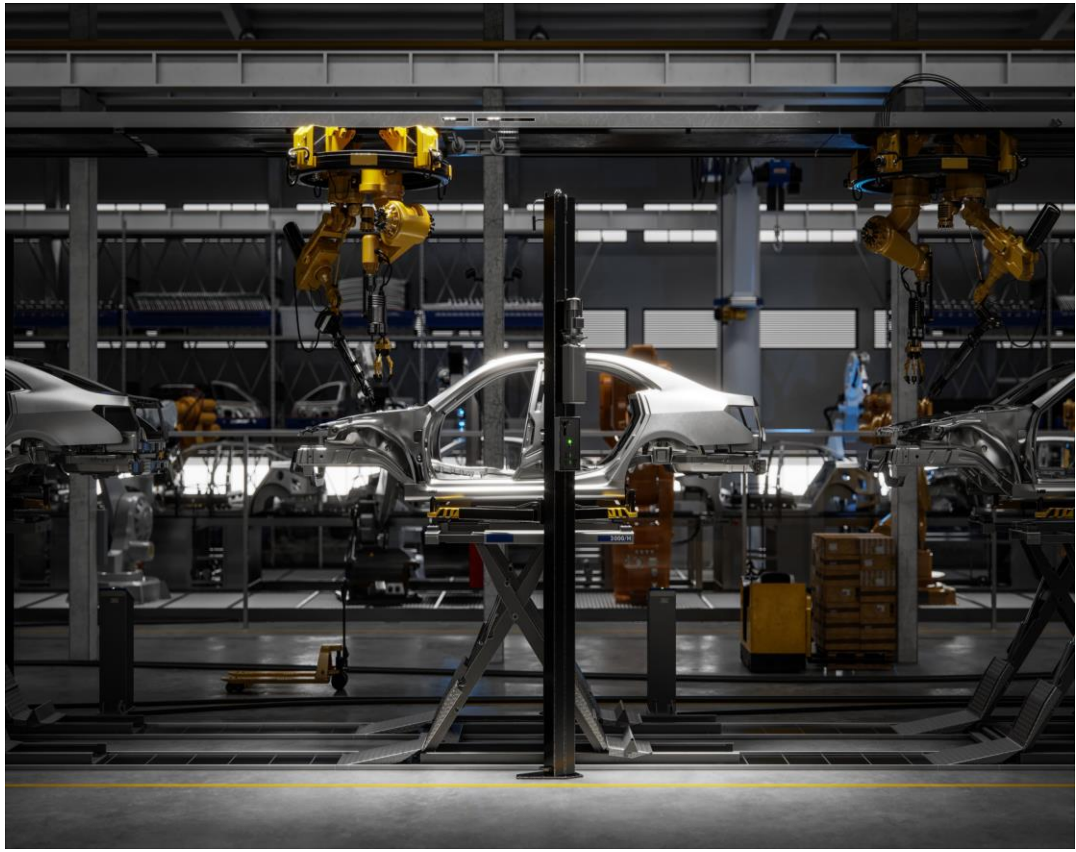
Trust Organization @ Autodesk

- **Trust Leader: Sebastian Goodwin**
  - **Security Design, Risk and Compliance Leader: George Ehrhorn**
  - **Security Risk Leader: Sapna Paul**
  - **GRC Lead: Clyde Tsai**
  - **Integration Partner: Estuate**

Security Org Strategic Intent

- **Customer Trust:** We build trust through execution of foundational security capabilities, guiding our organization’s adherence to compliance frameworks and introducing platform features that enhance our customer’s understanding of their security posture.
- **Secure by Default:** We enable secure by default through the definition and validation of standard processes and baselines deployed via automation.
- **Risk-Focused Priorities:** We create risk focused strategies by understanding the risk profiles within our company along with emerging trends across the world and apply these to guide our priorities.

Autodesk GRC Drivers



Maintaining FedRAMP Compliance

Compliance for ISO, SOC2, SOX ITGC, TISAX, C5, IRAP, Cyber Essentials

Lack of risk-aware decision making for our service/product owners

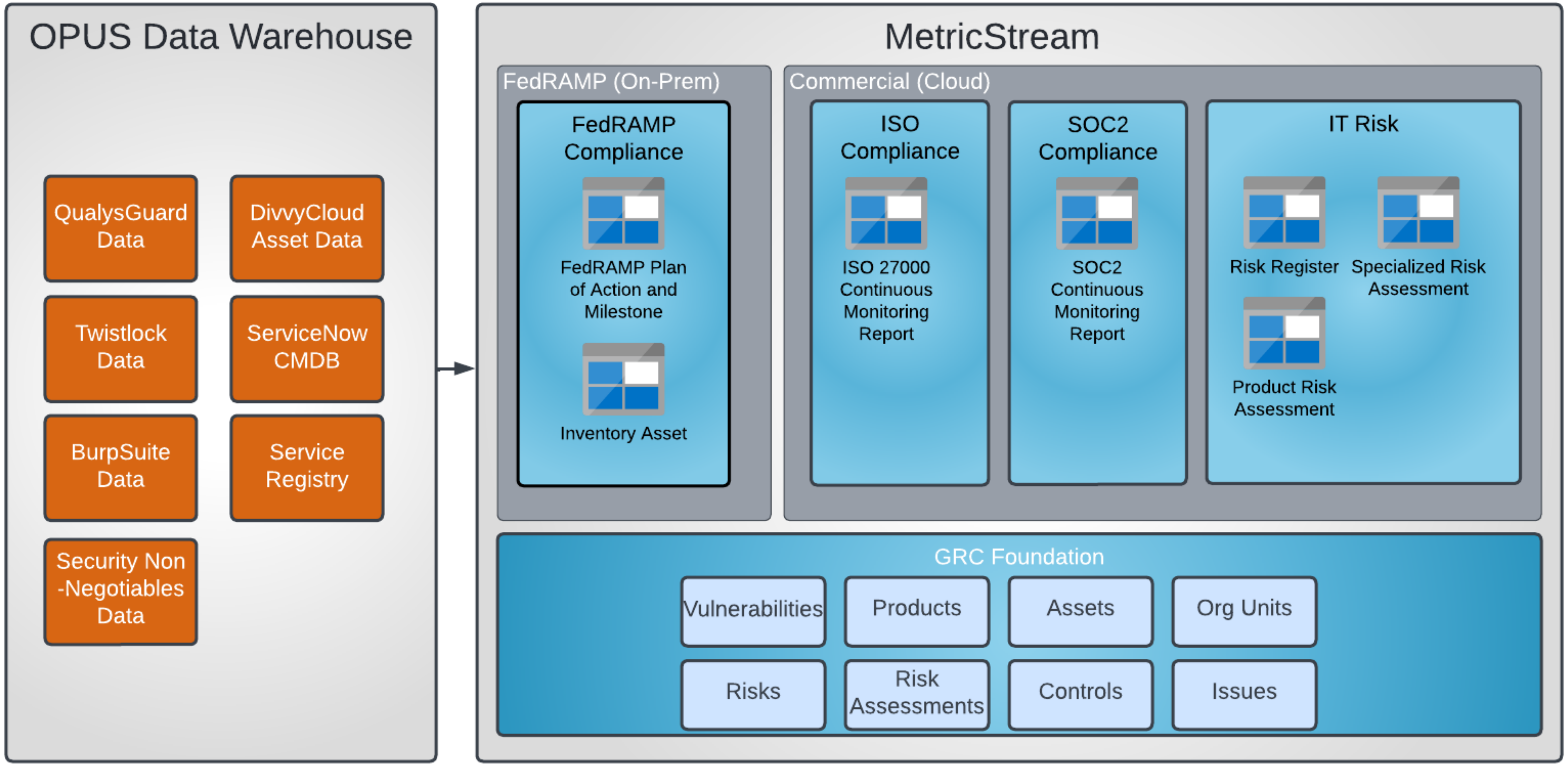
Limited resources for performing risk assessments

Lack of coordinated efforts between Risk, Compliance, Privacy, Security Operations, ERM, IA

Autodesk MS Journey

- Two years into our initial implementation
- IT Risk, IT Compliance, PDMS
- Owned by Security org, initial users are all in Security, now moving into broader Trust org
- Two instances: FedRAMP (on-prem) and Commercial (MS Cloud)

MetricStream - Current State



Business Value and Realized Benefits

- One stop for product owners and other leaders on SOC2 and ISO compliance
- Source of truth for risk register
- All security risk assessments performed from MetricStream
- Complete automation around FedRAMP Plan of Action and Milestones (POAM) tracking:
  - Generation of monthly POAM Report to sponsoring agency
  - Issues tracking for open vulnerabilities
  - Parity check to ensure more than 90% of assets are scanned
- Implemented integration framework and process for integrating all risk data from Opus data warehouse

MetricStream – Priorities for Next Year

- Priorities for next year
  - End-to-end compliance testing
  - Integrated Control Framework
  - Automated evidence collection
    - AWS, Azure, ServiceNow, DivvyCloud, etc
  - Policy Management Lifecycle

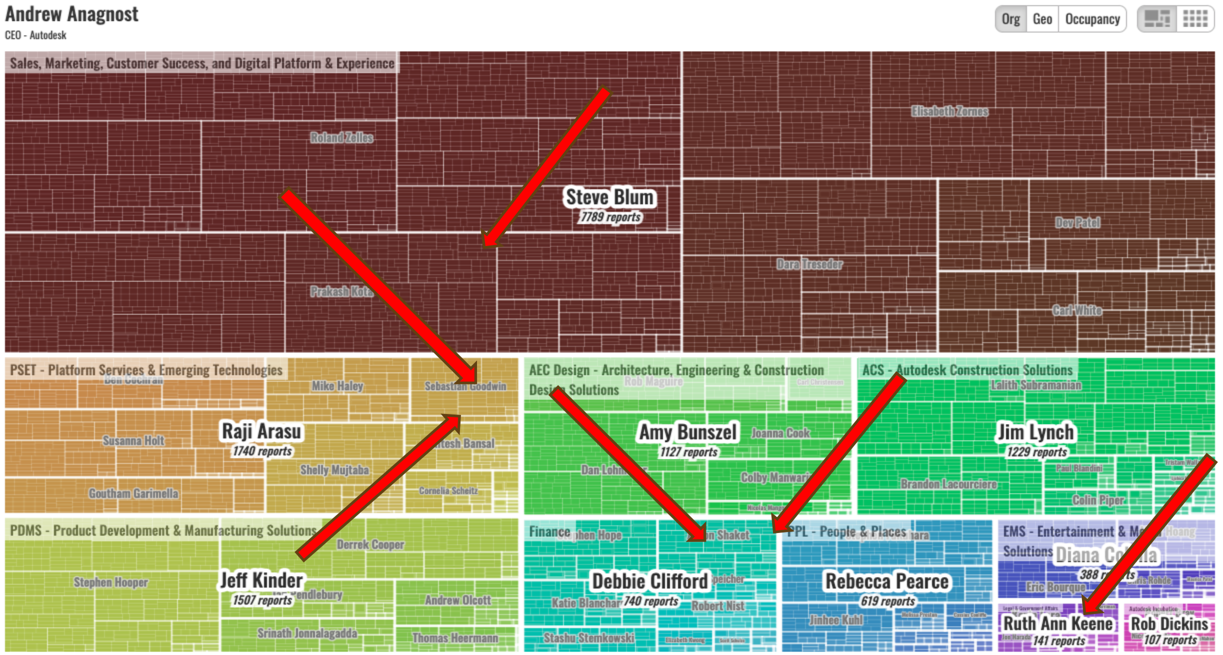
Top Challenges (*and Key Learnings*)

1. FedRAMP Compliance
   - Getting FedRAMP-moderate compliant
     - ~55 services/products in scope
     - 325 controls to implement
   - Two environments
     - FedRAMP (on-prem) and Commercial (cloud)
   - On-prem operations

   Understand the implications of FedRAMP segregation of data before technology design.

Top Challenges (*and Key Learnings*)

2. Silos!



Employ multi-channel communication wherever possible

Additional Challenges (*and Key Learnings*)

- Determining authoritative sources of truth for data

  Piggyback on other data consolidation efforts
- Getting new data sources into Opus timely

  Plan 2 quarters ahead
- Immature processes

  Opportunity to use technology to shape processes
- Immature ERM function

Questions?