Building a Security-First GRC Framework for Global Security Compliance

Rahat Sethi
Director, Technology GRC

Adobe

Agenda

Adobe’s Security & Compliance Strategy

Building a Security-First GRC Framework

Security Risk Management Framework

Policies & Standards

Security Controls Automation

Benefits of a Security-First GRC Framework

Adobe

29,000+

Employees in 37 countries

41+

Years of revolutionizing industries

$19.41B

FY2023 Revenue

"We are one of the largest and most diversified software companies in the world."

23

LEED Certifications

6000+

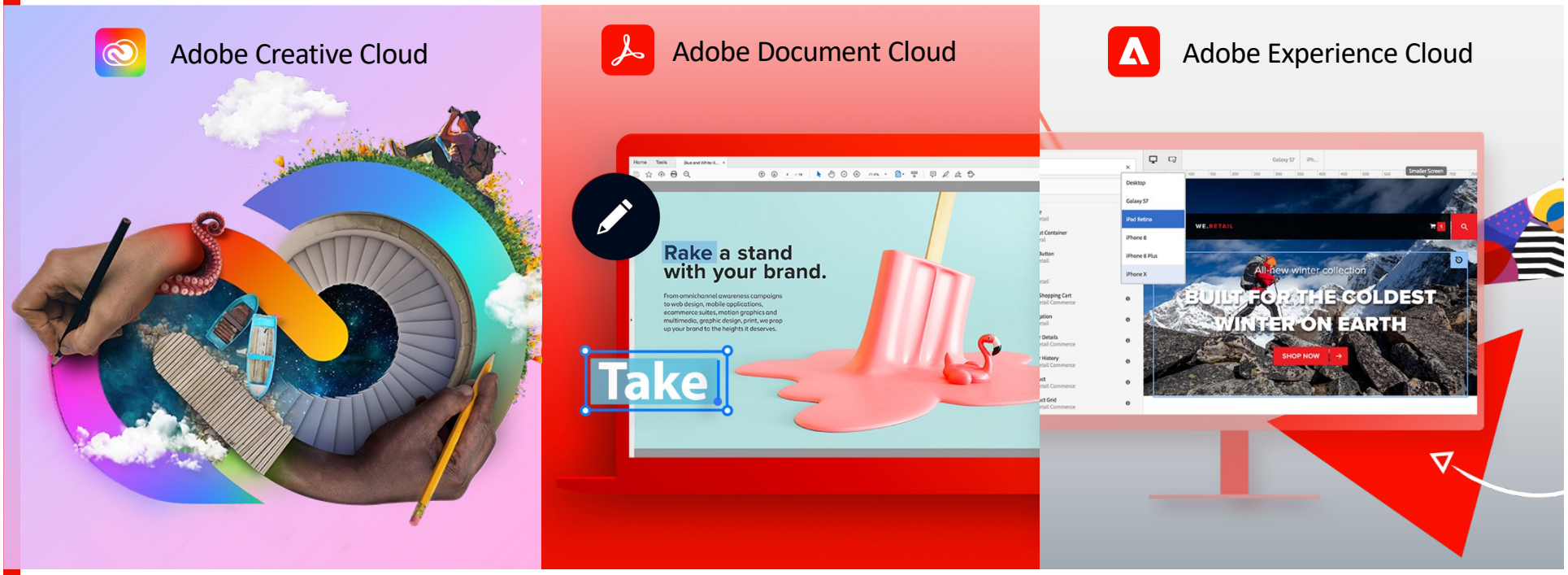
Patents

~$100M+

Given to the community in 2020

Adobe

Our Mission



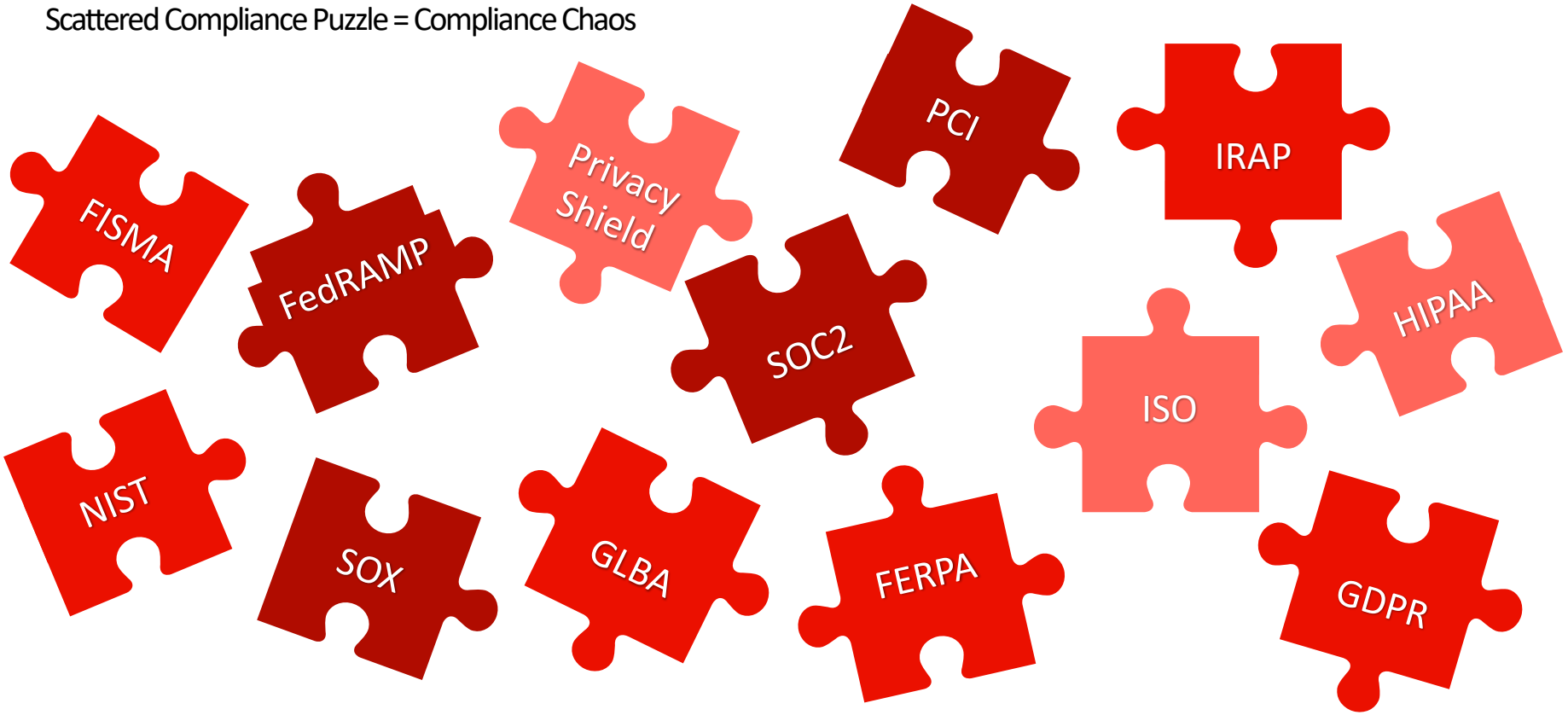
CONTENT ← - - - - - - - - - - → DATA

Adobe's Security & Compliance Strategy

Adobe

Solving the “Compliance Puzzle”

Scattered Compliance Puzzle = Compliance Chaos

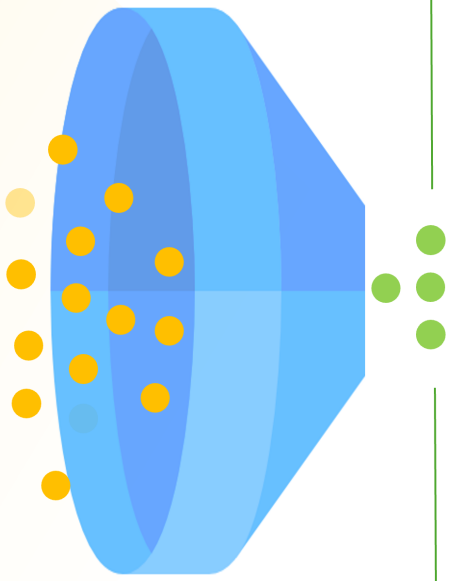


Common Controls Framework

Adobe's CCF V5.0

20+ Standards, ~4300 Control Requirements

- AICPA Trust Service Principles Service Organization Controls (SOC) - 40
- Cloud Computing Compliance Criteria Catalogue (BSI C5) - 120
- Cyber Essentials, UK - 24
- Critical Security Controls (CIS V8) - 150
- FedRamp Tailored & Moderate - 320
- Financial Security Institute CSP Evaluation, Korea - 56
- Health Information Portability and Accountability Act (HIPAA) - 70
- Infosec Registered Assessors Program, Australia (IRAP) - 880
- Information System Security Management and Assessment Program, Japan (ISMAP) - 1160
- ISO 27001:2022 & ISO 27002:2022 - 110
- ISO 27017:2015 - 7
- ISO 27018:2019 - 26
- ISO 22301:2019 - 200
- Monetary Authority of Singapore (MAS) - 230
- Multi-Layer Protection Scheme, China (MLPS) - 300
- NIST Cybersecurity - 100
- Payment Card Industry Data Security Standard (PCI DSS v4) - 290
- Spain Esquema Nacional de Seguridad (ENS) - 100
- TXRamp L1 - 120



314 Controls across 25 control domains

Asset Management	11
Backup Management	5
Business Continuity	6
Change Management	4
Configuration Management	15
Cryptography	15
Customer Managed Security	4
Data Management	21
Entity Management	11
Identity and Access Management	39
Incident Response	8
Mobile Device Management	4
Network Operations	18
People Resources	10
Privacy	10
Proactive Security	4
Risk Management	10
Security Governance	17
Service Lifecycle	7
Site Operations	16
System Design Documentation	2
Systems Monitoring	32
Third Party Management	13
Training and Awareness	9
Vulnerability Management	23

Building a Security-First GRC Framework

Adobe

Building a Security-First Framework

01 Driver-Subscriber-Contributor Model

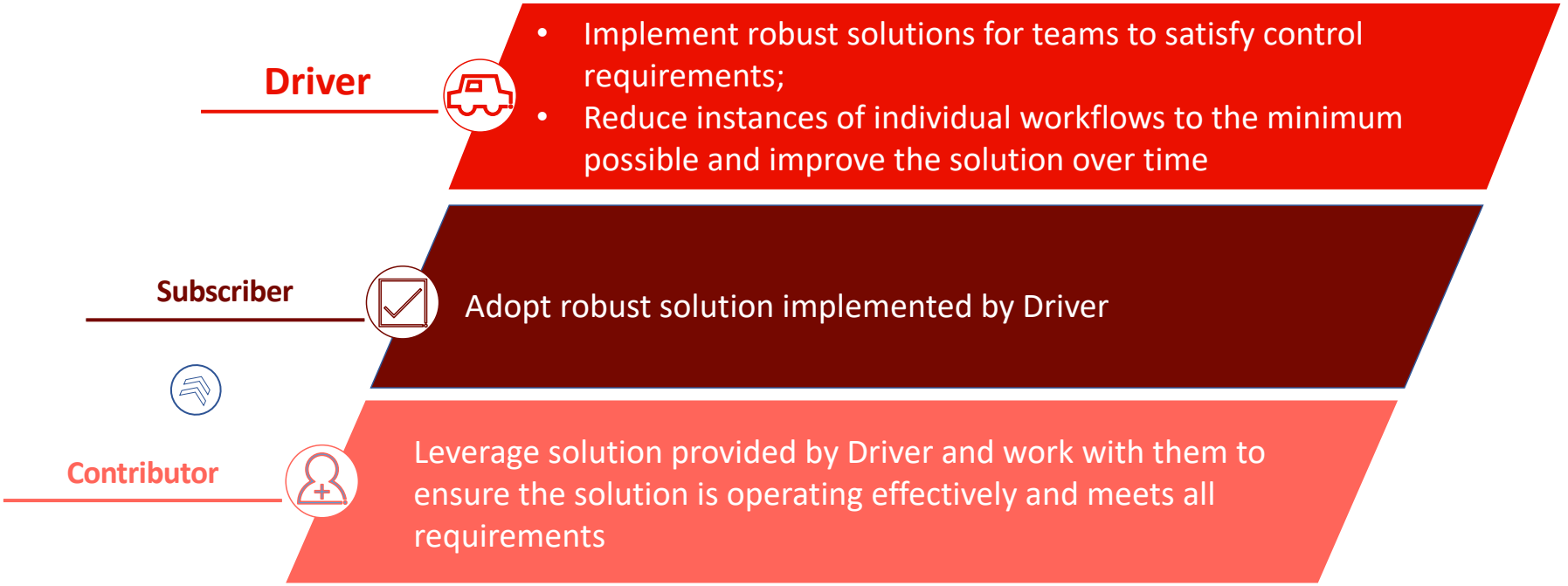
02 Risk Management Framework

03 Policies & Standards

04 Security Controls & Testing

05 Security Compliance Automation

Driver – Subscriber – Contributor Model



Establish a risk framework and methodology for risk evaluation

Define a consistent risk terminology across Security

Build comprehensive risk rating criteria that allows for meaningful measurement and easy comparison

Establish a risk management framework that unifies Security by delivering *consistent*, *data-driven*, and *meaningful* results.

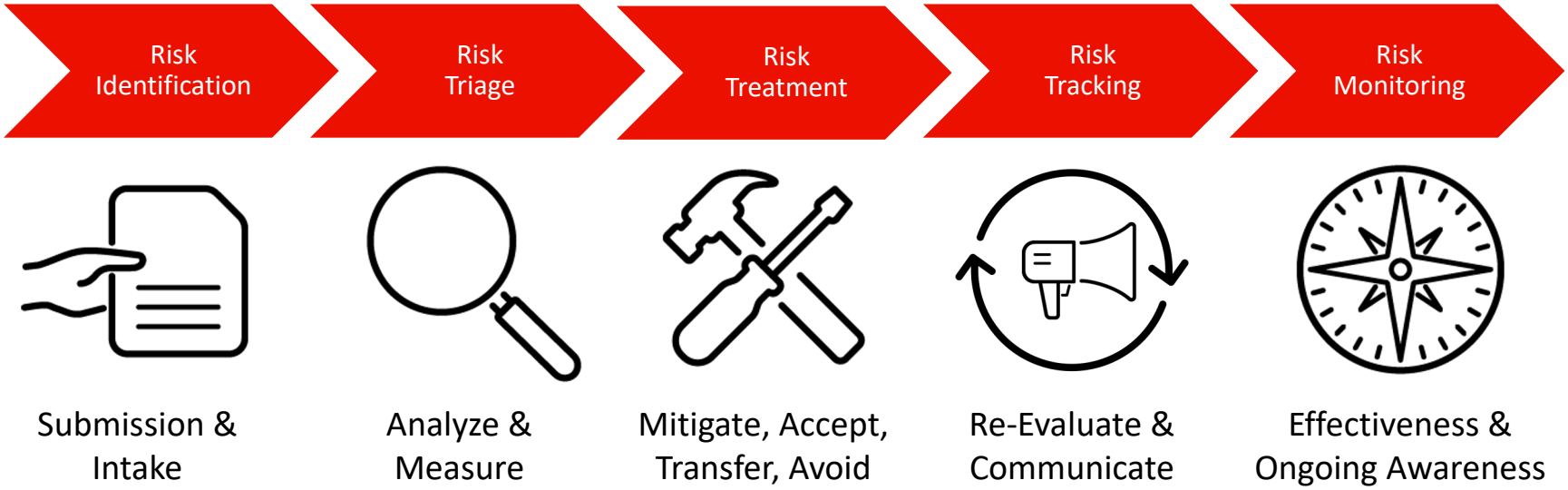
Create a Unified Risk Register to identify and track priorities

Communicate risk results to enable Management to make well-informed decisions

Partner with Business and Product teams in risk reduction efforts

Adobe

Risk Lifecycle



Policies & Standards

Persona-Based Structure

Clear & Concise

Data Driven

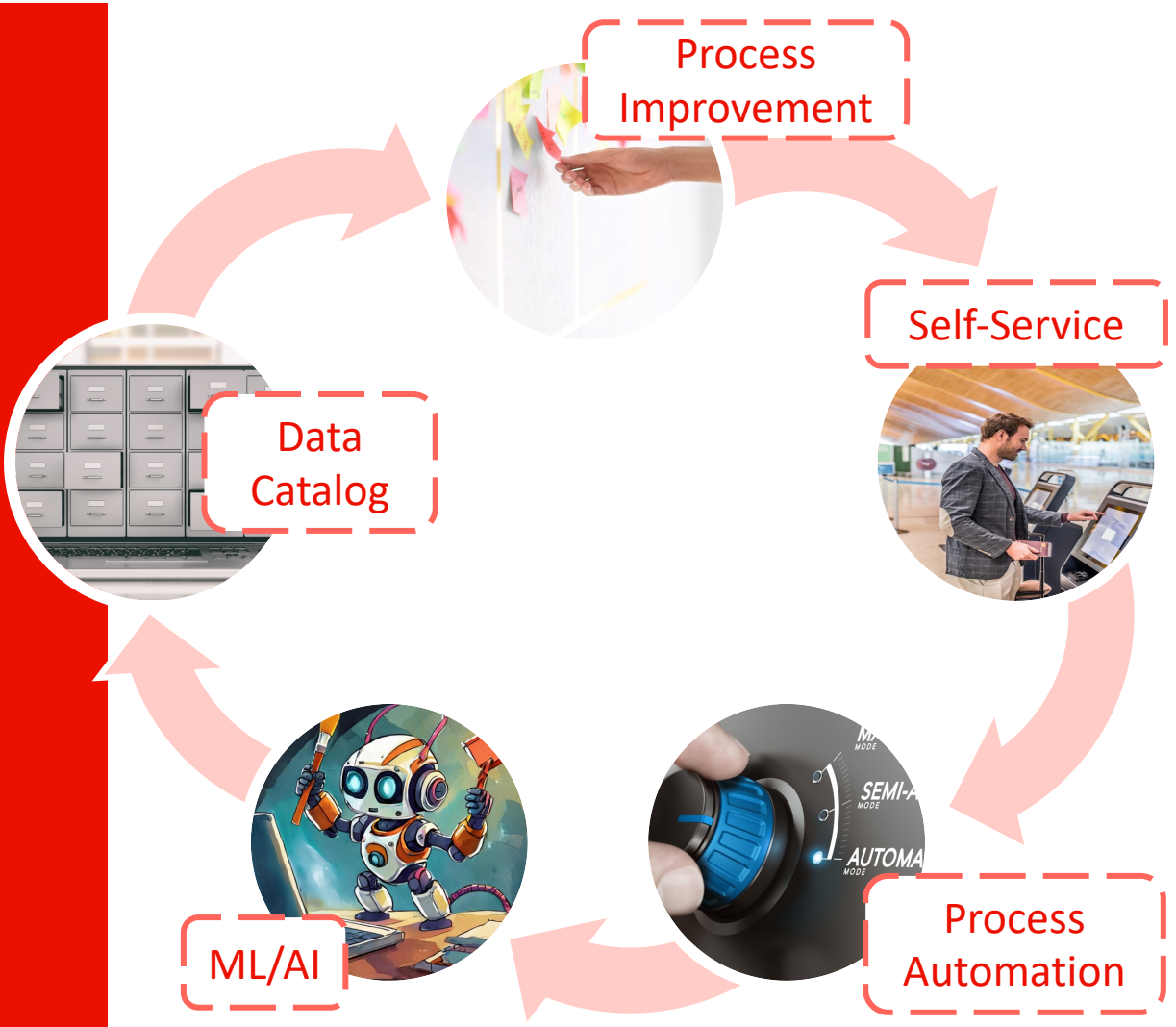
Reporting & Monitoring

Control Automation:

Increase GRC *scalability*, *trust*, and *continuous monitoring* while reducing **compliance fatigue**.

Adobe

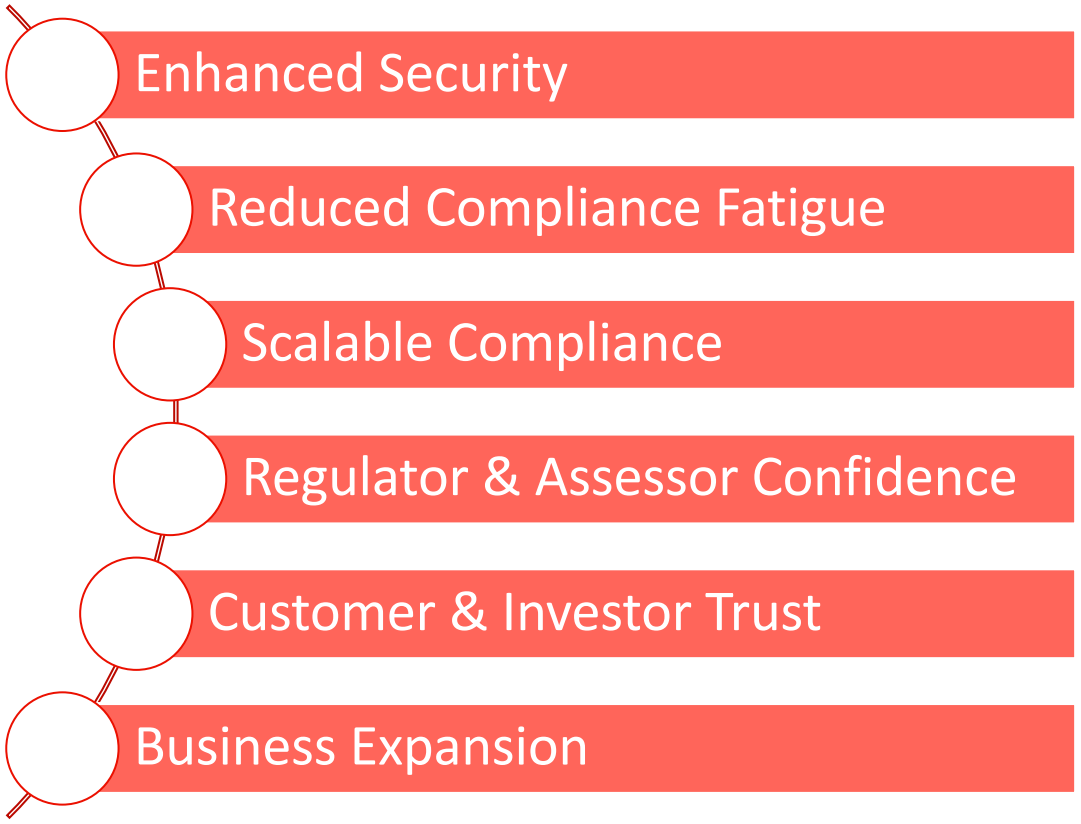
Steps to Build Towards Control Automation



Benefits of a Security-First GRC Framework

Adobe

Benefits of a Security-First Framework



Thank You

Rahat Sethi
Director, Tech GRC

Learn more about Adobe's CSO Award-winning ***Security Risk Management Framework*** *tomorrow @ 11:15AM in the digital poster program hall.*

Adobe