3M: Best Practices for a Successful ABAC Deployment

KT Mahmudi, SAP Security and Access Manager, 3M
Keng Lim, CEO, NextLabs
Session ID #83016

May 7 – 9, 2019

About the Speakers

Keng Lim

- CEO, NextLabs
- Launched and built several software companies including Kiva Software, Netscape, Escalate, and Sygate over the last 20 years

KT Mahmudi

- SAP Security & Access Manager, 3M
- CISSP, CCSP with 15 years of experience in Access Control

ASUG

Key Outcomes/Objectives

1. Learn how 3M leveraged SAP DAM to protect trade secrets and address other access-control-related use cases

2. Learn how 3M made its decision on a vendor

3. Learn best practices on how to ensure a successful ABAC deployment

ASUG

Agenda

- Intros
- Current Trends
- Key Challenges
- About 3M
- Solution & Selection Process
- Implementation
- Results
- Q&A

Current Trends

- **All About the Data**
  - Data is everywhere and fueling the digital economy
  - When coupled with security, it can be a competitive advantage

- **Security Remains a Top Concern**
  - Intellectual property theft & attacks by nation-states
  - IoT (Internet of Things) devices a new vector for data breaches

- **Ever-changing Regulatory Landscape**
  - Several compliance mandates (export controls, NIST)
  - Privacy issues (GDPR)

ASUG

Core Customer Challenges

"How do I manage the balance between **providing the access** necessary to run the business, while ensuring that my **data is secure** and the **business is within compliance**?"
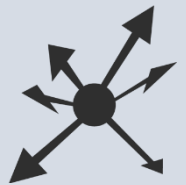
Need to Share

Collaboration

- Globally distributed workforce
- External partners
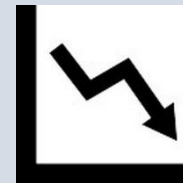- Distributed supply chains

Business Agility

- Time-to-market acceleration
- Business process transformation
- IT consolidations & migrations
- Corporate restructurings (M&A, JVs, divestitures)

Need to Protect

Risk Reduction

- Secure sensitive data
- Protect critical IP
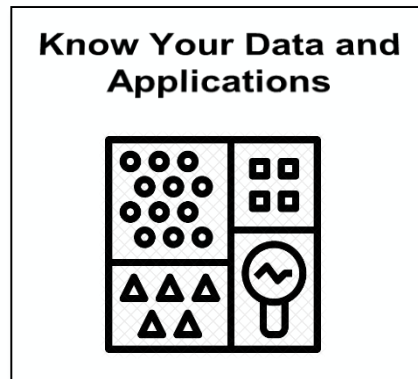- Prevent data breaches
- Secure supply chains

Governance & Compliance

- Comply with regulations (GDPR, ITAR, SOX, etc.)
- Avoid penalties
- Centralize reporting & audits

A Modern, Risk-Based Approach to Security Is Key

A sound security program should be predicated on an understanding of risk within a business context.

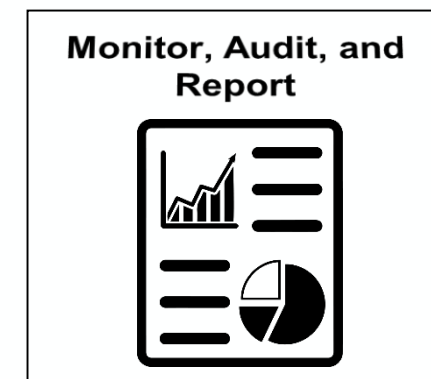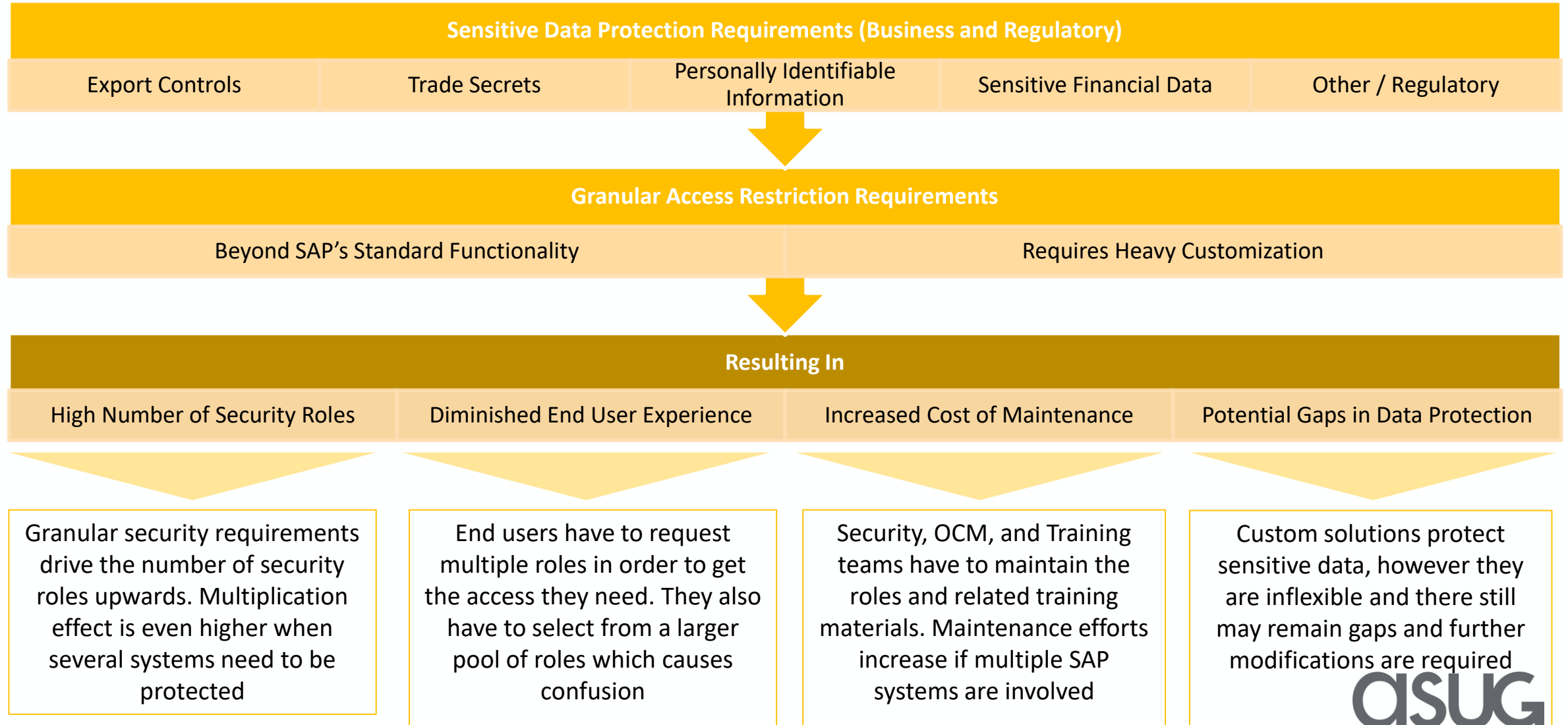| Know Your Data and Applications	Protect Data at the Source	Protect Data on the Move	Monitor, Audit, and Report
Know what kinds of data you have, where it's stored, and what safeguards are in place to protect that data	Control and enforce access policies to data within applications	Apply rights management to files and documents as they are shared internally and externally	Continuously monitor security events, audit user activities, and report as needed

ASUG

THE 3M STORY

About 3M

- Global powerhouse, our products improve the daily lives of people around the world

- More than 60,000 3M products are used in homes, businesses, schools, hospitals and other industries

- Industries we operate in include: Safety & Industrial, Transportation & Electronics, Health Care, and Consumer

- 91,000 employees across 70 countries

Scaling OOTB Security Capabilities Has Challenges

Issues and Drivers

Sensitive Data Protection Requirements (Business and Regulatory)

Export Controls	Trade Secrets	Personally Identifiable Information	Sensitive Financial Data	Other / Regulatory

Granular Access Restriction Requirements

Beyond SAP's Standard Functionality	Requires Heavy Customization

Resulting In

High Number of Security Roles	Diminished End User Experience	Increased Cost of Maintenance	Potential Gaps in Data Protection
Granular security requirements drive the number of security roles upwards. Multiplication effect is even higher when several systems need to be protected	End users have to request multiple roles in order to get the access they need. They also have to select from a larger pool of roles which causes confusion	Security, OCM, and Training teams have to maintain the roles and related training materials. Maintenance efforts increase if multiple SAP systems are involved	Custom solutions protect sensitive data, however they are inflexible and there still may remain gaps and further modifications are required

aSUG

Capability Assessment

Capability Comparison Between Custom Solution and ABAC

Item	Custom Solution (as-Is)	Custom Solution (fully implemented)	ABAC
Improved Overall Data Protection, Compliance, and Auditability	★☆☆☆	★★★☆	★★★☆
Reduction in Number of Security Roles	★★☆☆	★★☆☆	★★★☆
Improved End User Experience	★★☆☆	★★☆☆	★★★☆
Ease of Transaction Code Modifications in the Future	★☆☆☆	★☆☆☆	★★★★
Reduction of Complications Related to BOM Authorization Group Proliferation and Permutations	★★☆☆	★★★☆	★★★★

★★★★ Best   ★★★ Good   ★★ Average   ★ Limited

asug

Capability Assessment (cont'd)

Capability Comparison Between Custom Solution and ABAC

Item	Custom Solution (as-Is)	Custom Solution (fully implemented)	ABAC
Centralized Authorization Engine For Multiple Systems	☆☆☆☆	☆☆☆☆	★★★☆
Potential Future Integration with Legacy and Other Applications	☆☆☆☆	☆☆☆☆	★★★☆
Availability of SAP Product Support	★☆☆☆	★☆☆☆	★★★★
Attestation And Access Re-Certification	★☆☆☆	★★☆☆	★★★☆

★★★★ Best   ★★★ Good   ★★ Average   ★ Limited

ASUG

Our ABAC Journey

Prior to 2017
- Plant-based security
- Worldwide roles
- Standard SAP functionality

Customization
- Customize standard SAP transactions
- Geolocation

ABAC Eval.
- Capability Assessment
- Vendor Selection
- Position paper

NextLabs
- Licensed NextLabs
- Project scope
- Approach to secure data

NextLabs Pilot
- Q3 2018
- Plant
- Technology
- Bills of Material
- Recipes

asUG
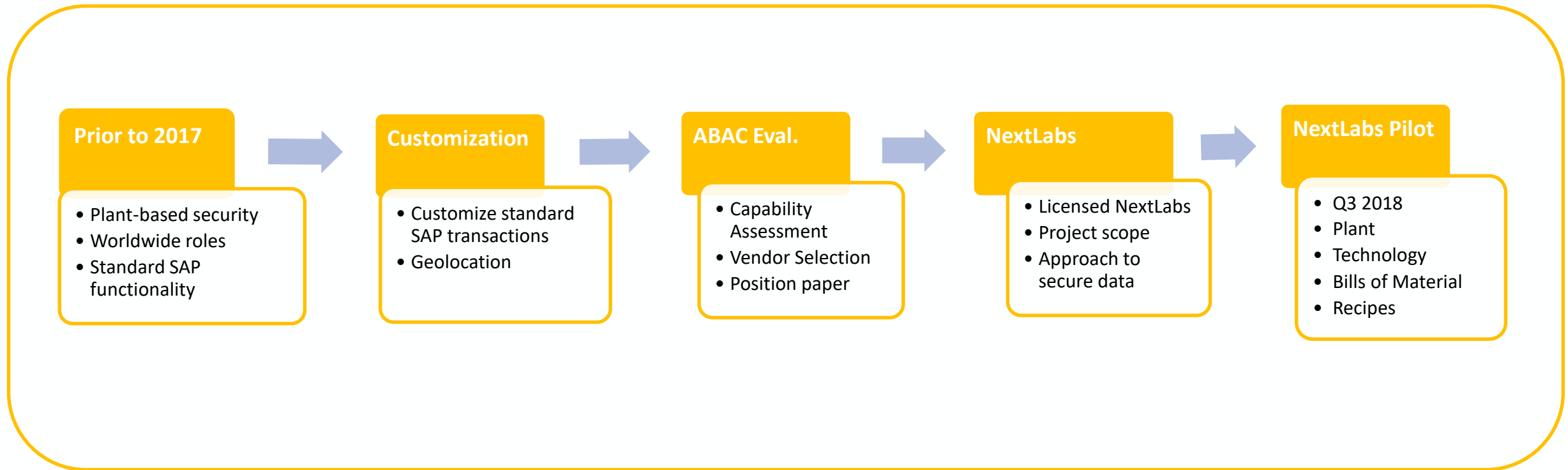
Pilot Implementation

Infrastructure
- 7 NextLabs environments
- NextLabs add-on installed on ECC
- Linux and Oracle

Plant
- Technology
- Single Trade Secret Attribute

Transactions
- 23 SAP Transactions
- BOMs and Recipes

Requirements
- 6 Requirements
- 2 WRICEFs
- 2,000 users

Pilot Approach
- Identify and read attributes of trade secret materials
- Identify and read attributes off plant users
- Define policy allowing and denying access to trade secrets

ASUG

Results - Value Realized from ABAC

Value Drivers

Efficiency - Enables automatic enforcement of business rules and policies

Risk Mitigation - Complies with regulatory requirements associated with foreign export control jurisdictions

Risk Mitigation - Provides real-time monitoring for insight into data access and helps prevent data leaks
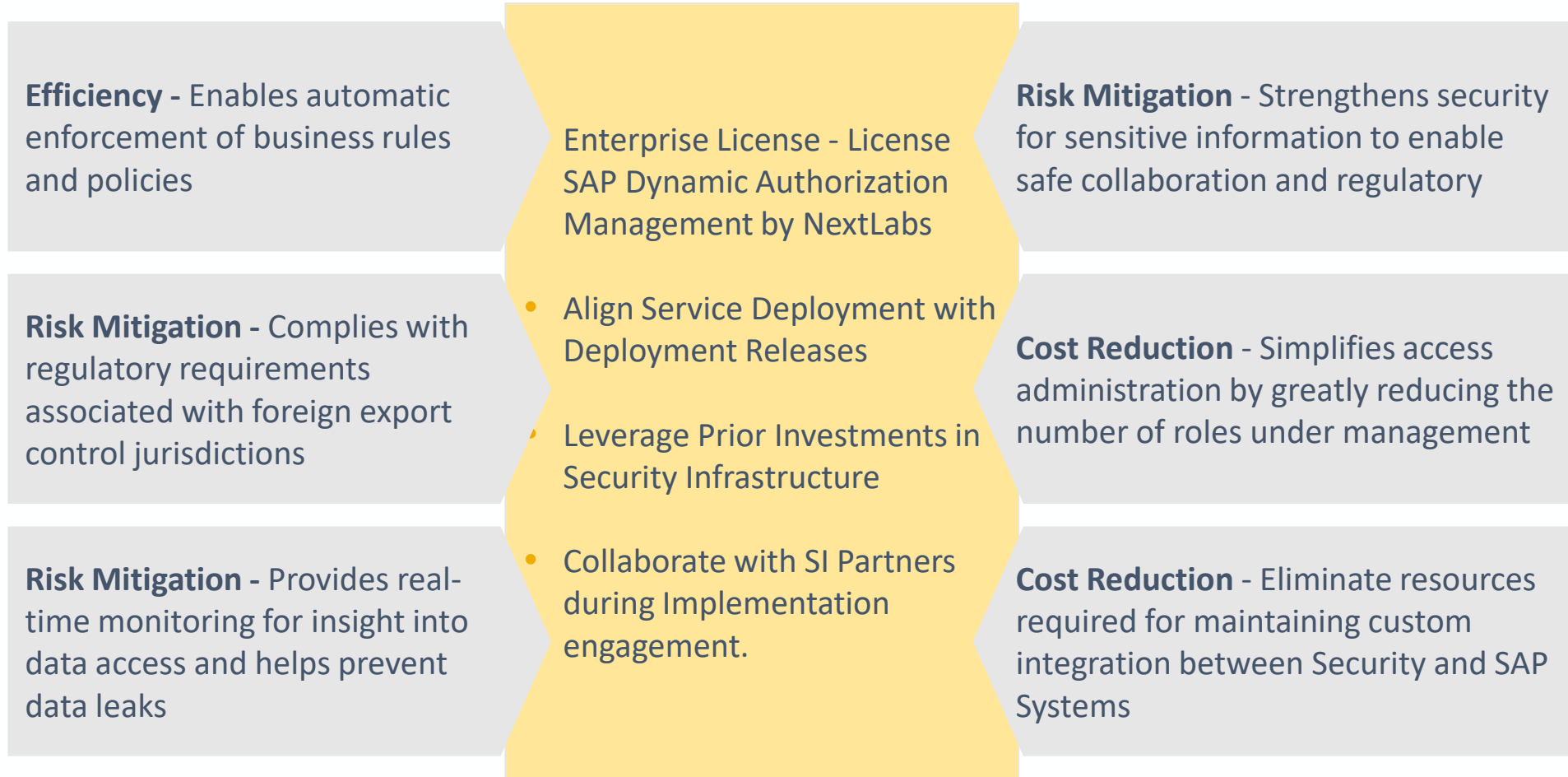
Enterprise License - License SAP Dynamic Authorization Management by NextLabs

- Align Service Deployment with Deployment Releases

- Leverage Prior Investments in Security Infrastructure

- Collaborate with SI Partners during Implementation engagement.

Risk Mitigation - Strengthens security for sensitive information to enable safe collaboration and regulatory

Cost Reduction - Simplifies access administration by greatly reducing the number of roles under management

Cost Reduction - Eliminate resources required for maintaining custom integration between Security and SAP Systems

Our ABAC Future Projects

2019 Q2-Q3
- Fiori Batch Mgmt.
- Fiori QM
- Fiori Print Label
- Table Browser Transactions

2019 Q4
- 17 plants w TS
- Bills of Material
- Recipes
- Inspection Plants
- Quality Results
- Usage Decision
- UI
- Sub Contractors

Future Wishlist
- MES Integration
- Equipment
- Documents
- Retrofit
- Enovia
- Export Control
- EWM
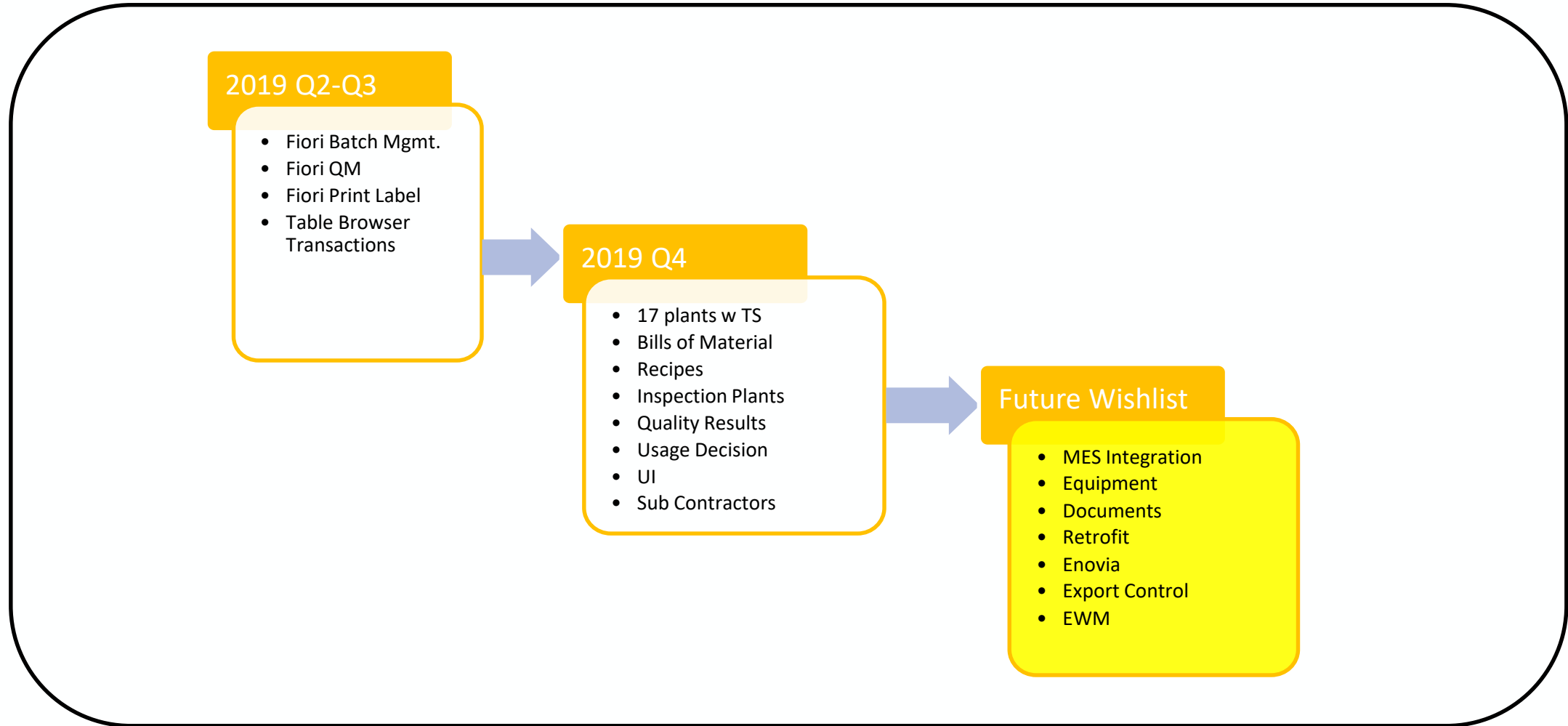
Take the Session Survey.

We want to hear from you! Be sure to complete the session evaluation on the SAPPHIRE NOW and ASUG Annual Conference mobile app.

ASUG

Presentation Materials

Access the slides from 2019 ASUG Annual Conference here:
http://info.asug.com/2019-ac-slides

ASUG

Q&A

For questions after this session, contact us at keng.lim@nextlabs.com and kmahmudi@mmm.com.

Let's Be Social.

Stay connected. Share your SAP experiences anytime, anywhere.
Join the ASUG conversation on social media: **@ASUG365 #ASUG**

ASUG