



TRUSTING THE PROCESS:

Real-life Lessons on How Change Management
and Communications are Essential for Zero Trust

Sarah Chu Villarmarzo
MA, PMP, CISSP, ITIL4, SAFe Agilist

Purpose & Objectives

The purpose of this session is to translate best practices from real-world communications and change management experience into successful Zero Trust transitions.

Learning Areas:


- ✓ The Importance of Communication
- ✓ Understanding Your Stakeholders
- ✓ Communication Types
- ✓ Emphasizing Zero Trust Benefits
- ✓ Internal vs. External Change Management
- ✓ Use Case: Going Passwordless

Change Management

Change management is your organization's approach to identifying, rolling out, and sustaining changes, from a people perspective.

Use change management to:

- + Help your people understand changes and impacts
- + Improve predictability at every stage
- + Increase buy-in and user adoption
- + Provide a feedback loop on changes



It's critical to approach change holistically and proactively, especially for changes that are complex or impact many users – think Zero Trust or enterprise identity updates.

Communication in Change Management

Because communication is the very foundation of successful change management, it should always be:



Multi-Lateral



Proactive



Transparent



Tailored*

**Remember: always know your audience!*

Don't Trust – Communicate.

What Can Go Wrong



- x Low User Adoption
- x Confusion from Users
- x Shadow IT
- x Service Interruptions

These effects have the potential to be very public!

What Can Go Right



- + User Buy-In
- + Change Champions
- + Smooth Rollouts
- + More Transparency, Less Risk

In short: all of the benefits for Zero Trust, only expanded.

Engaging Stakeholders

Who are they?



+ Map Them Out

Who are they and how will ZT changes affect them?

+ Continual Updates

A living doc that informs both comms and policies

What do they do?



+ Know Your Users

Pay attention to user types, roles, and access needs

+ Policy Maintenance

Make regular updates and keep ZT teams informed

What do they think?



+ Pain Points

Find automation opportunities, serve comms needs, etc.

+ Better Product

Deeper insights will improve product/solution/rollout

What do they need?



+ Communications

Translate needs into different communication types

+ Timeline

Develop a schedule/ roadmap for training, etc.

Communication Types



Announcements



Training



Press Releases



Focus Groups



Surveys



Reference Sites

**Begin with
WHAT and WHY.
Then get into
WHEN and HOW.**

Internal vs. External

Internal and external stakeholder have different change needs.

Internal Stakeholders:

- + Two-way dialogue
- + Communicate early & often
- + Part of the design process
- + Internal materials and policies



External Stakeholders:

- + One-way, more controlled
- + Finalized information
- + Limit sensitive information
- + Public sources for reference



USE CASE: GOING PASSWORDLESS

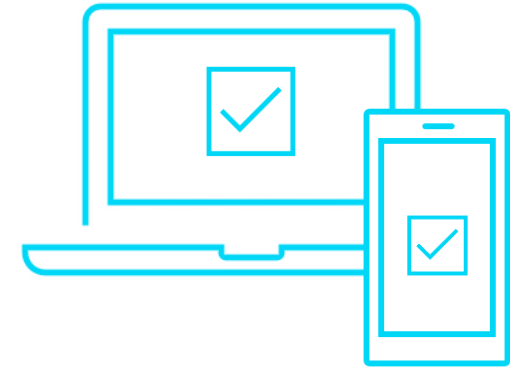
Use Case: Passwordless MFA Rollout

Business Need:

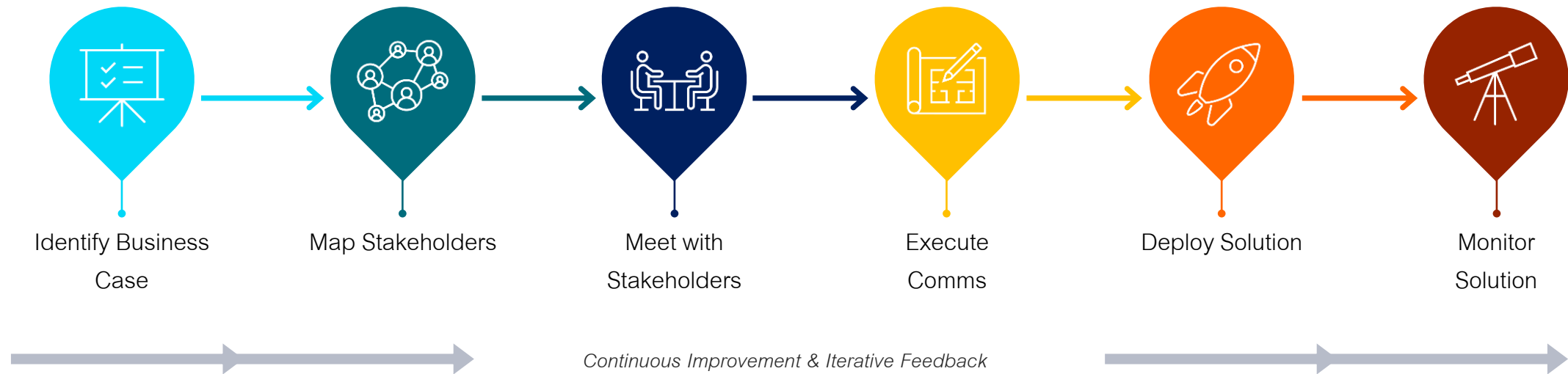
- ☑ Passwordless MFA solution for enterprise users: compliance and security
- ☑ Users of public-facing applications: passwordless option

Considerations:

- + Timeline & compliance needs
- + Security needs
- + Maturity of IT infrastructure
- + User demographics



Managing the Change



SUMMARY

Leading Practices

- ✓ Plan ahead
- ✓ Check for materials that already exist
- ✓ Tailor it to your audience and their needs
- ✓ Use plain language
- ✓ Highlight the benefits
- ✓ Keep an open door



THANK YOU!

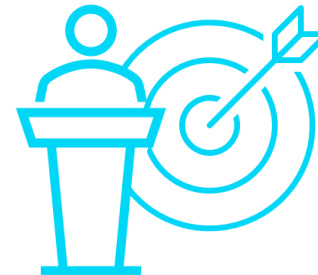
Abstract

Technical leaders understand the importance of adopting Zero Trust models in an ever-changing cyber threat landscape. But getting users on board, whether enterprise or consumers, can be a different story. Zero Trust changes the way users interact with system components, through stronger authentication, tighter access control, stricter device and data governance, and more. Users may struggle to understand new usage patterns, leading to help desk floods, frustration, and attempts to circumvent security measures.

This session will provide best practices from real-world change management experiences, giving guidance on communicating in plain language about the importance of your changes, emphasizing the benefits of your approach, and preparing your organization for a smooth transition. The session features a use case of an organization rolling out passwordless authentication.

This session will help participants:

- + Understand foundational concepts of organizational change management
- + Enhance their ability to prepare for and manage changes related to Zero Trust
- + Improve organizational practices for communications
- + Maximize the effectiveness of zero trust changes



Bio & Contact



Sarah Chu Villarmarzo

MA, PMP, CISSP, ITIL4, SAFe Agilist

Sarah Chu Villarmarzo is a Senior Manager with Easy Dynamics, a cloud, identity, and cybersecurity services firm based in McLean, VA. She has over 10 years of experience providing strategic consulting to federal clients, notably IRS cybersecurity and fraud prevention, DHS identity and access management, and HHS emerging technology. Ms. Villarmarzo specializes in consulting and implementation of identity proofing, anti-fraud, federation, and zero trust networks. Ms. Villarmarzo holds a B.A. in political science and management and an M.A. from American University. She has been recognized for her community service work, winning the Heroines of Washington Rising Star award for her program teaching computer skills to refugee students. She is a regular contributor to thought leadership organizations such as ACT-IAC, the Kantara Initiative, and more.

svillarmarzo@easydynamics.com

