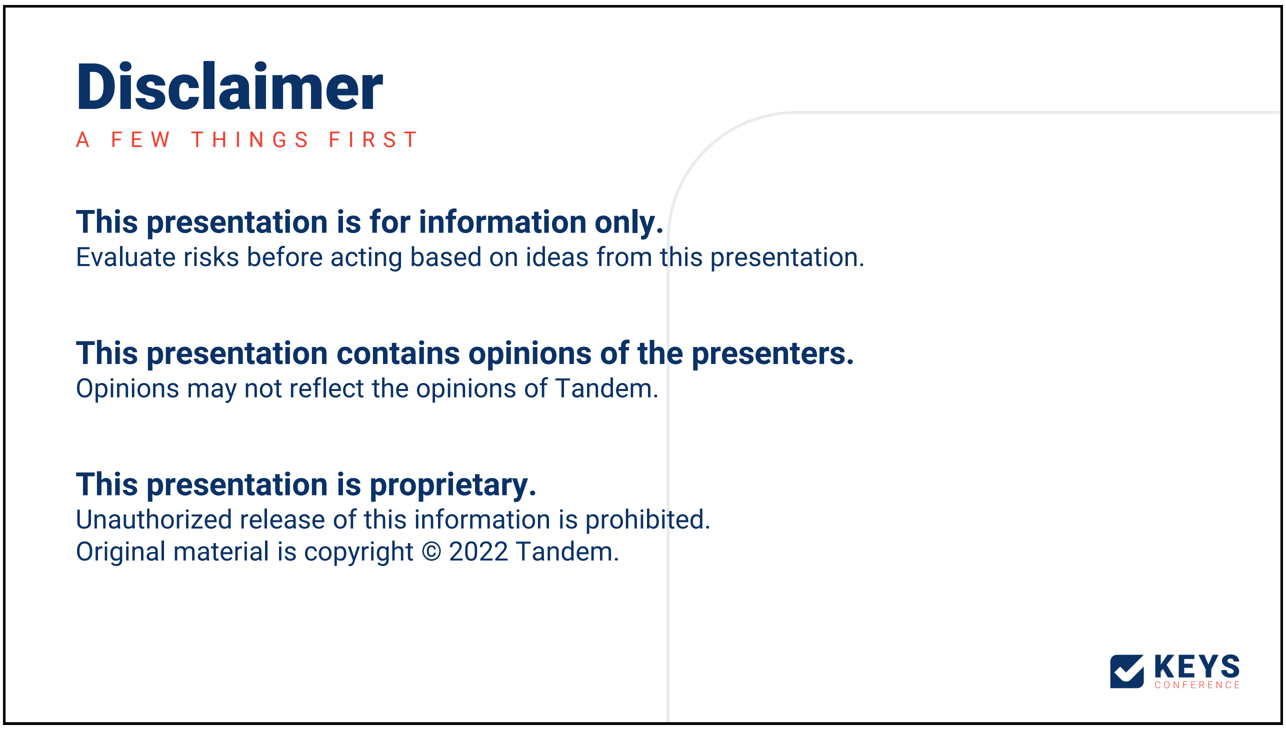
Bret Mills and Missy Oliver

How to Address the Most Frequently Found Security Issues

KEYS CONFERENCE

1



Disclaimer

A FEW THINGS FIRST

This presentation is for information only.
Evaluate risks before acting based on ideas from this presentation.

This presentation contains opinions of the presenters.
Opinions may not reflect the opinions of Tandem.

This presentation is proprietary.
Unauthorized release of this information is prohibited.
Original material is copyright © 2022 Tandem.

KEYS CONFERENCE

2

3

Bret Mills

Audit and Security Consultant

Missy Oliver

Compliance and Information Consultant

CRVPM III

4

Security Issues

1 Compliance

2 Network/Vulnerabilities

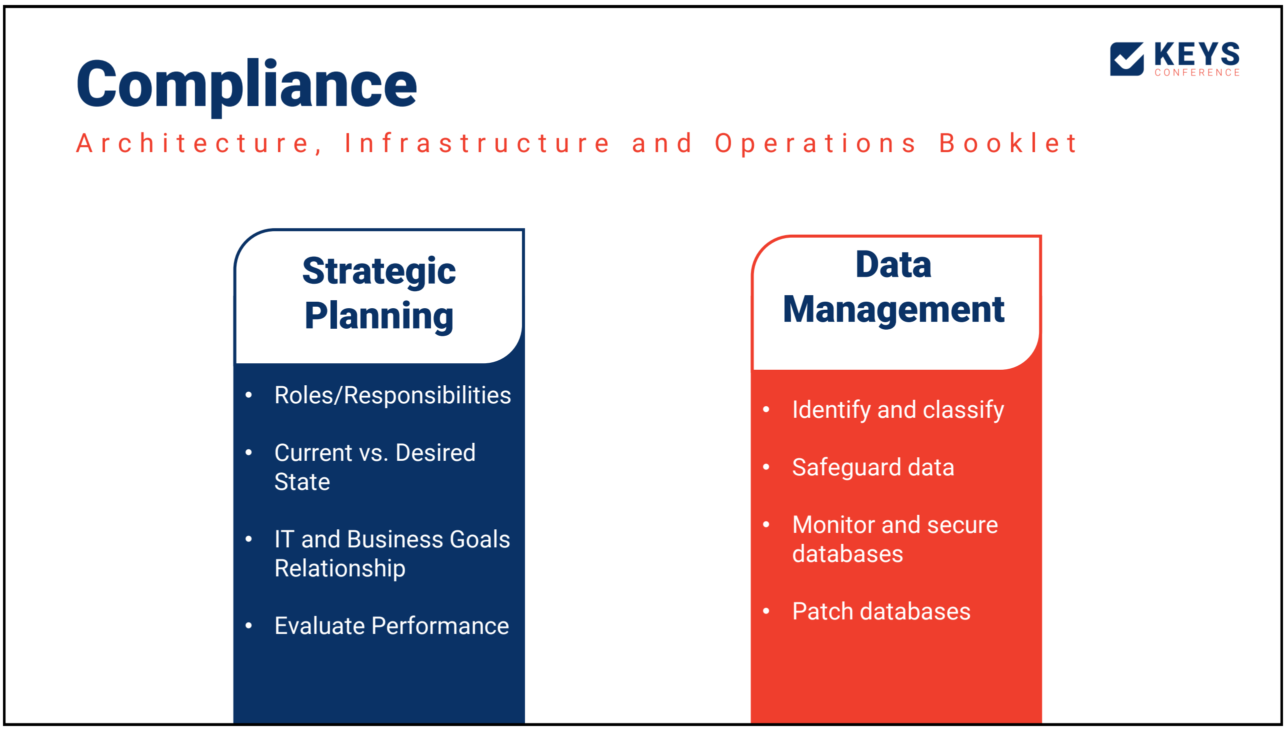
3 Moving Forward Tips

5

COMPLIANCE

Security Issues addressed in new guidance.

6



Compliance

Architecture, Infrastructure and Operations Booklet

Strategic Planning

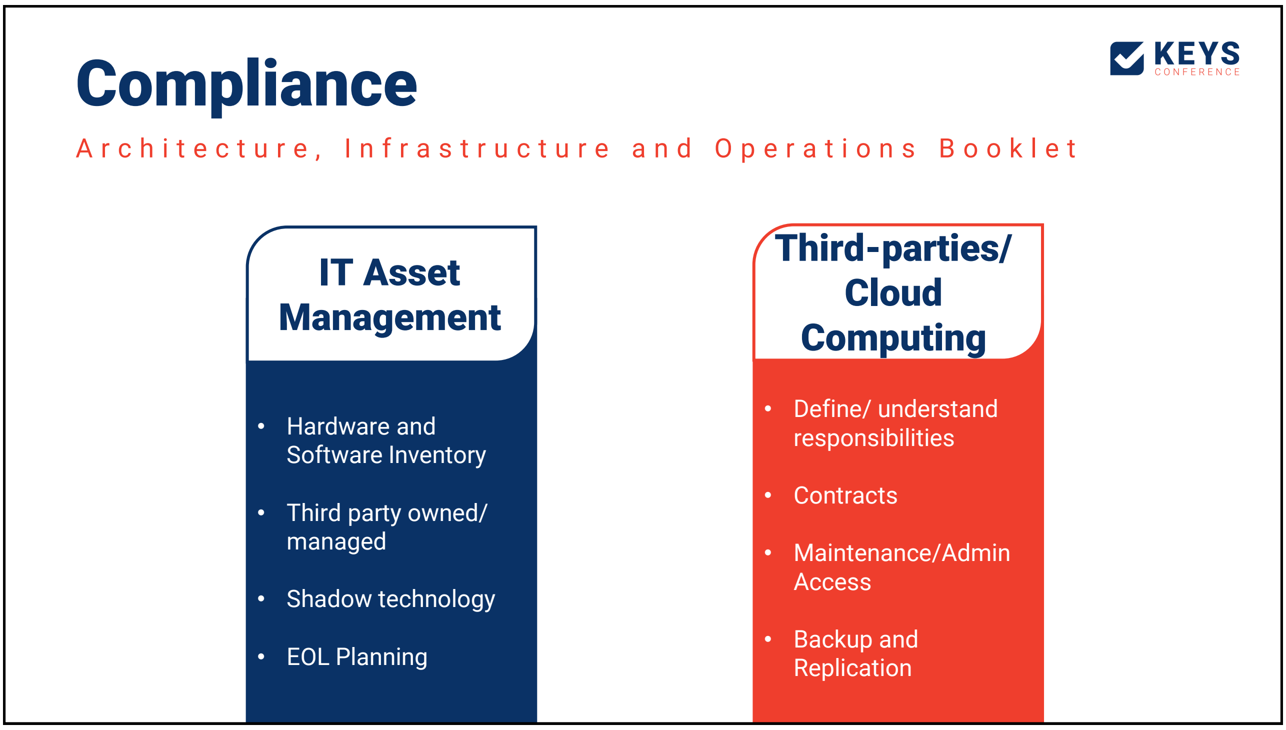
- Roles/Responsibilities
- Current vs. Desired State
- IT and Business Goals Relationship
- Evaluate Performance

Data Management

- Identify and classify
- Safeguard data
- Monitor and secure databases
- Patch databases

KEYS CONFERENCE

7



Compliance

Architecture, Infrastructure and Operations Booklet

IT Asset Management

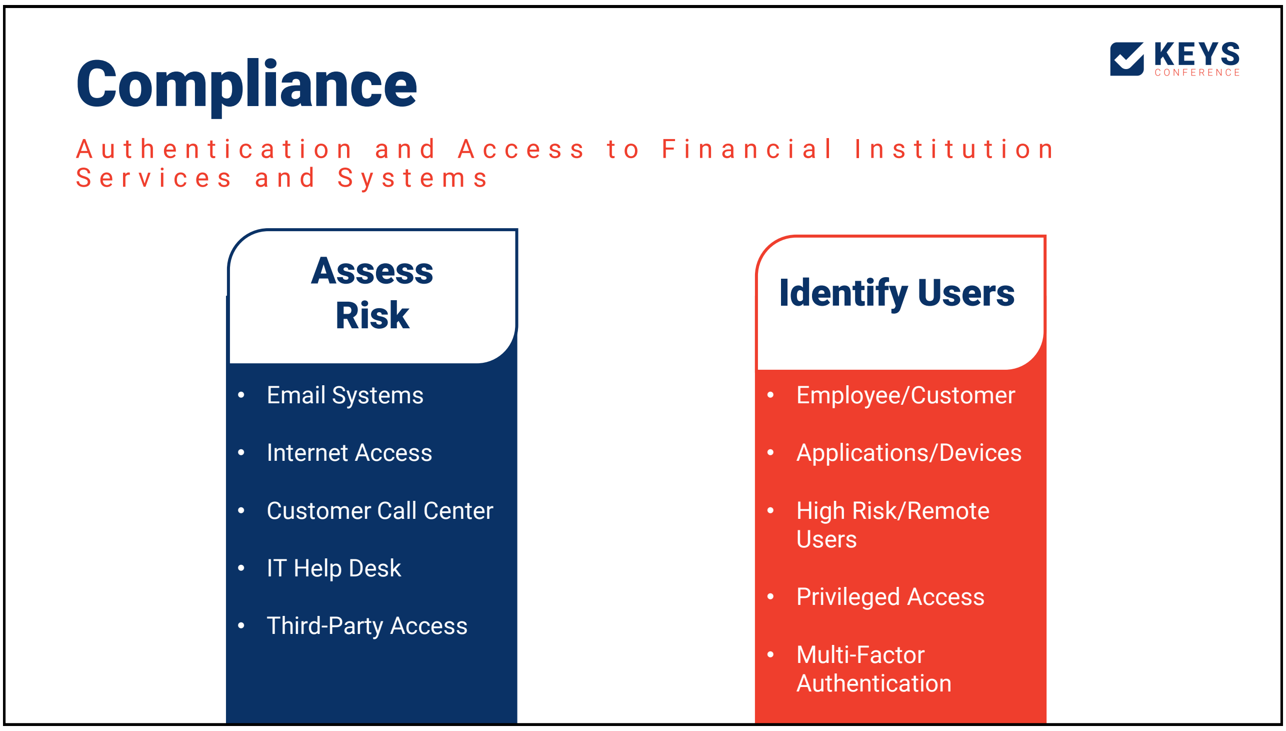
- Hardware and Software Inventory
- Third party owned/ managed
- Shadow technology
- EOL Planning

Third-parties/ Cloud Computing

- Define/ understand responsibilities
- Contracts
- Maintenance/Admin Access
- Backup and Replication

KEYS CONFERENCE

8



Compliance

Authentication and Access to Financial Institution Services and Systems

Assess Risk

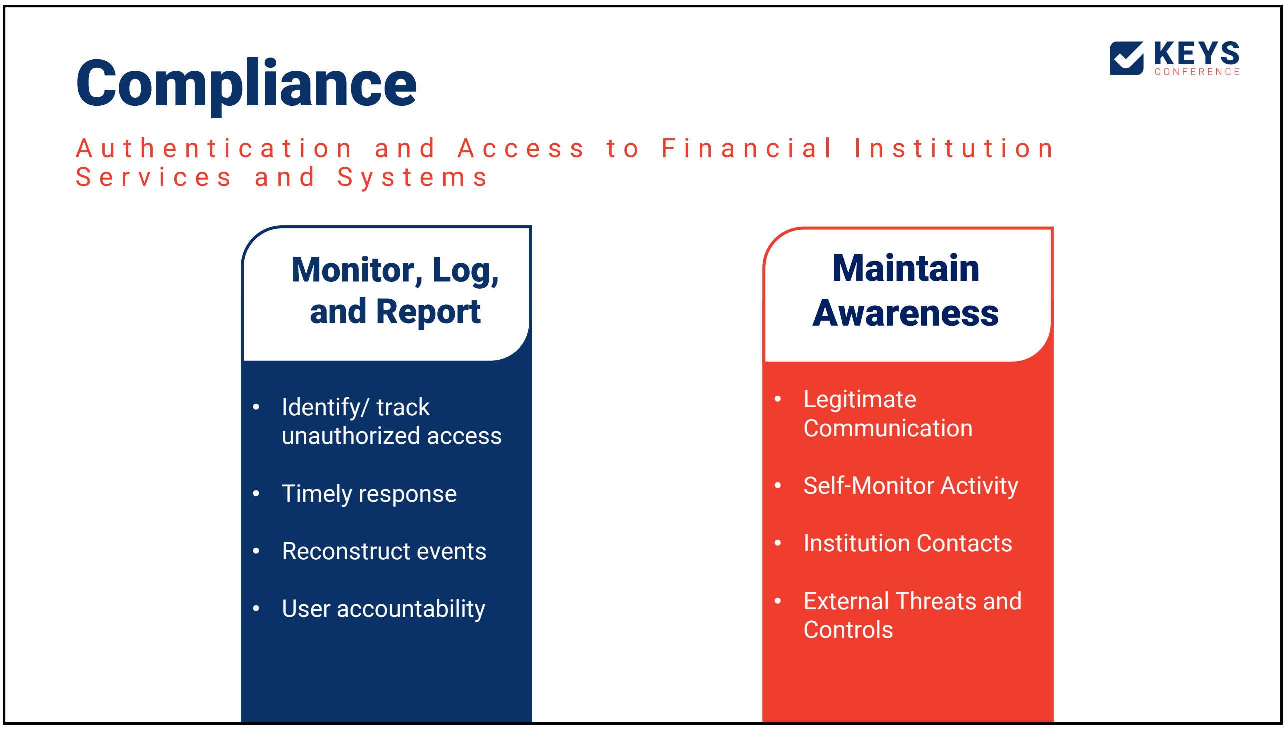
- Email Systems
- Internet Access
- Customer Call Center
- IT Help Desk
- Third-Party Access

Identify Users

- Employee/Customer
- Applications/Devices
- High Risk/Remote Users
- Privileged Access
- Multi-Factor Authentication

KEYS
CONFERENCE

9



Compliance

Authentication and Access to Financial Institution Services and Systems

Monitor, Log, and Report

- Identify/ track unauthorized access
- Timely response
- Reconstruct events
- User accountability

Maintain Awareness

- Legitimate Communication
- Self-Monitor Activity
- Institution Contacts
- External Threats and Controls

KEYS
CONFERENCE

10

Compliance

Incident Management

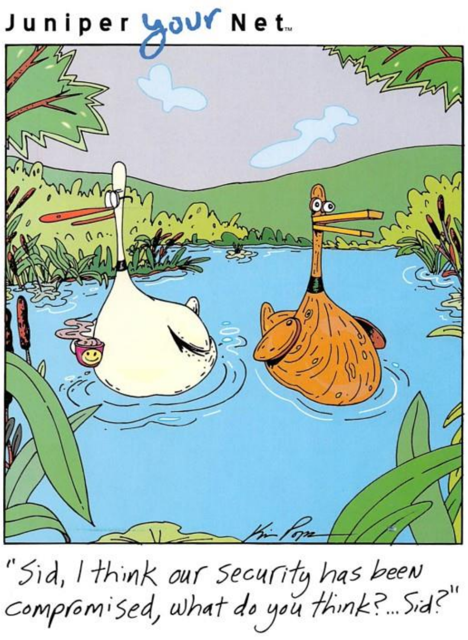
1 Incident Notification

2 Chain of Custody

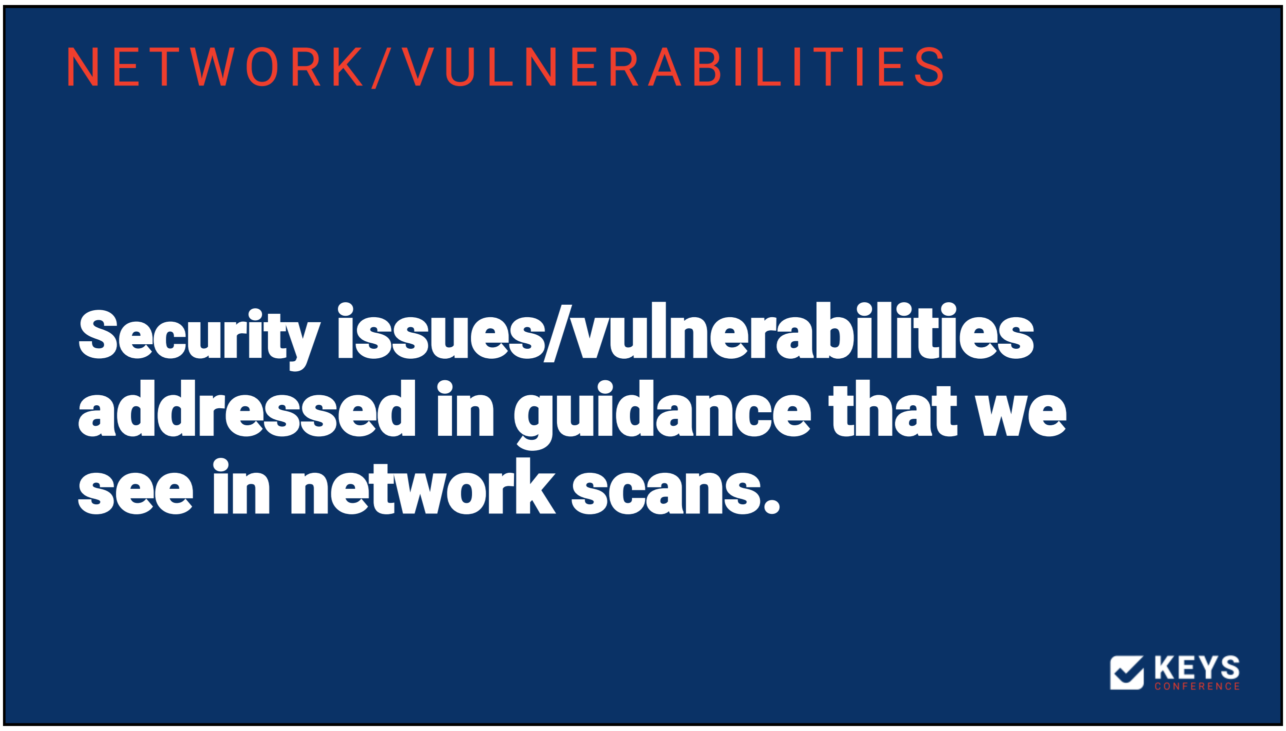
3 Forensic Investigation

4 Contact Information

11


Juniper your Net™
"Sid, I think our security has been compromised, what do you think?... Sid?"

12



NETWORK/VULNERABILITIES

Security issues/vulnerabilities addressed in guidance that we see in network scans.

KEYS CONFERENCE

13

Network

1 Patch Management

2 Unsupported Software

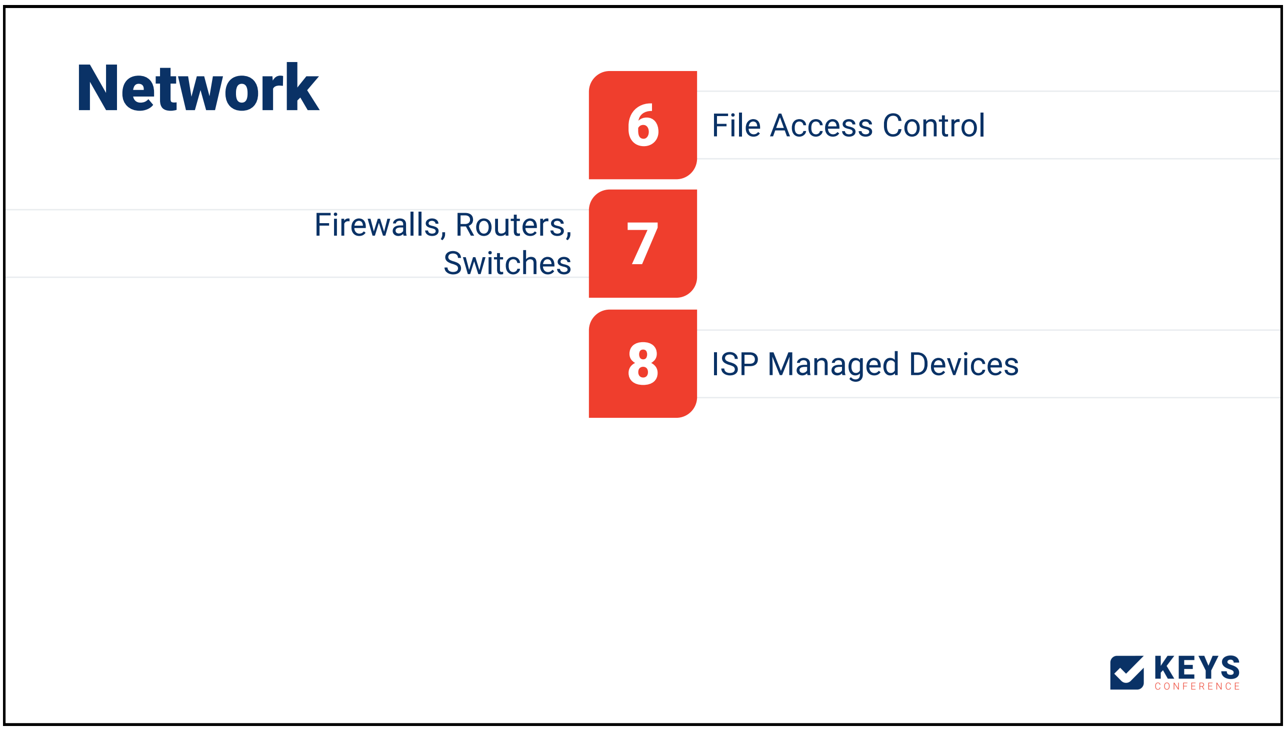
3 Legacy Systems

4 Unnecessary Accounts on the Network

5 Unnecessary Services and Protocols

KEYS CONFERENCE

14



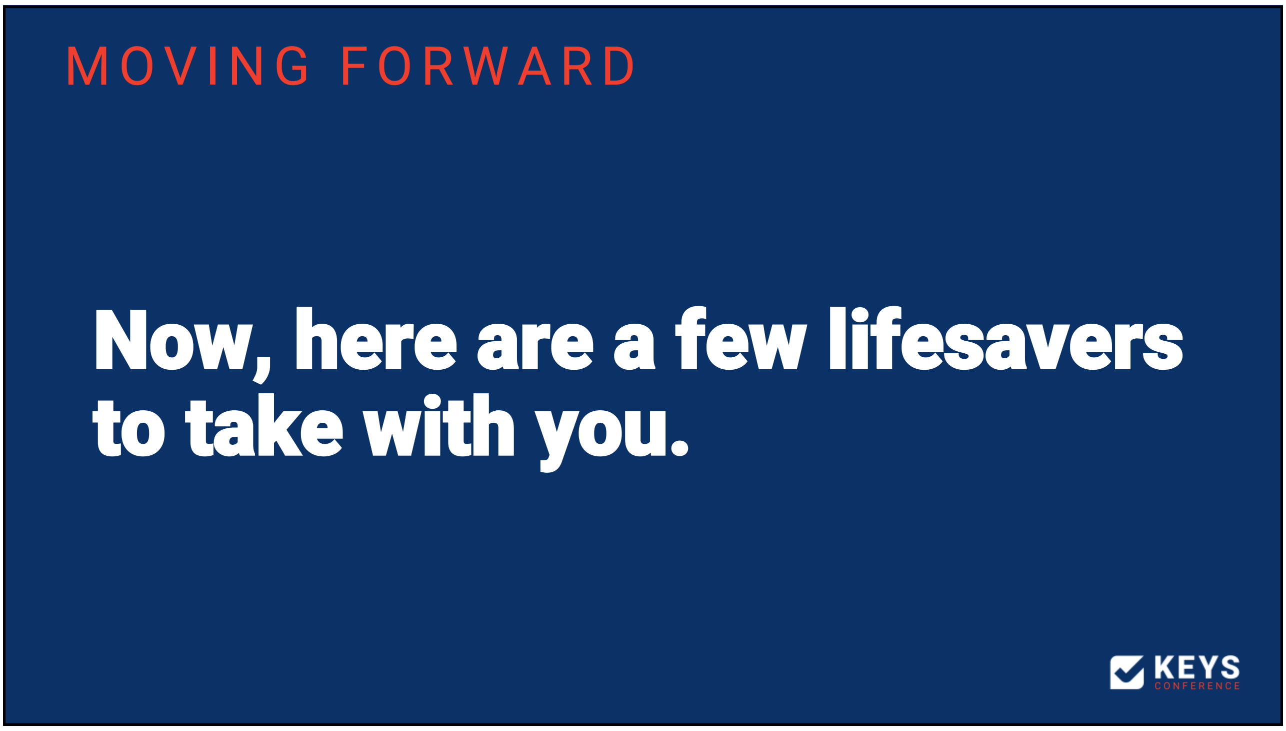
Network

6 File Access Control

Firewalls, Routers, Switches 7

8 ISP Managed Devices

15



MOVING FORWARD

Now, here are a few lifesavers to take with you.

16

Moving Forward

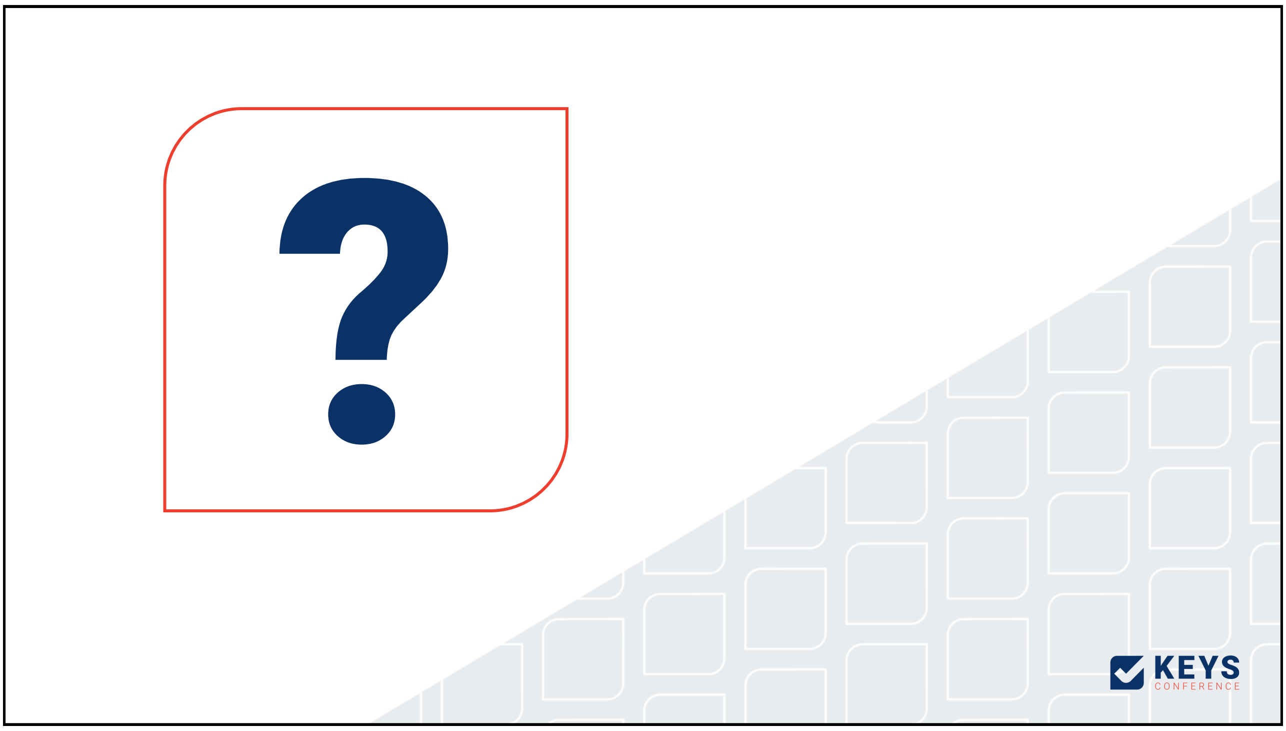
Now what do we do?

1. Communicate
2. Who is Mitigating Issues?
3. Understand Audit/Exam Findings
4. Document, Document, Document
5. Validate, Validate, Validate

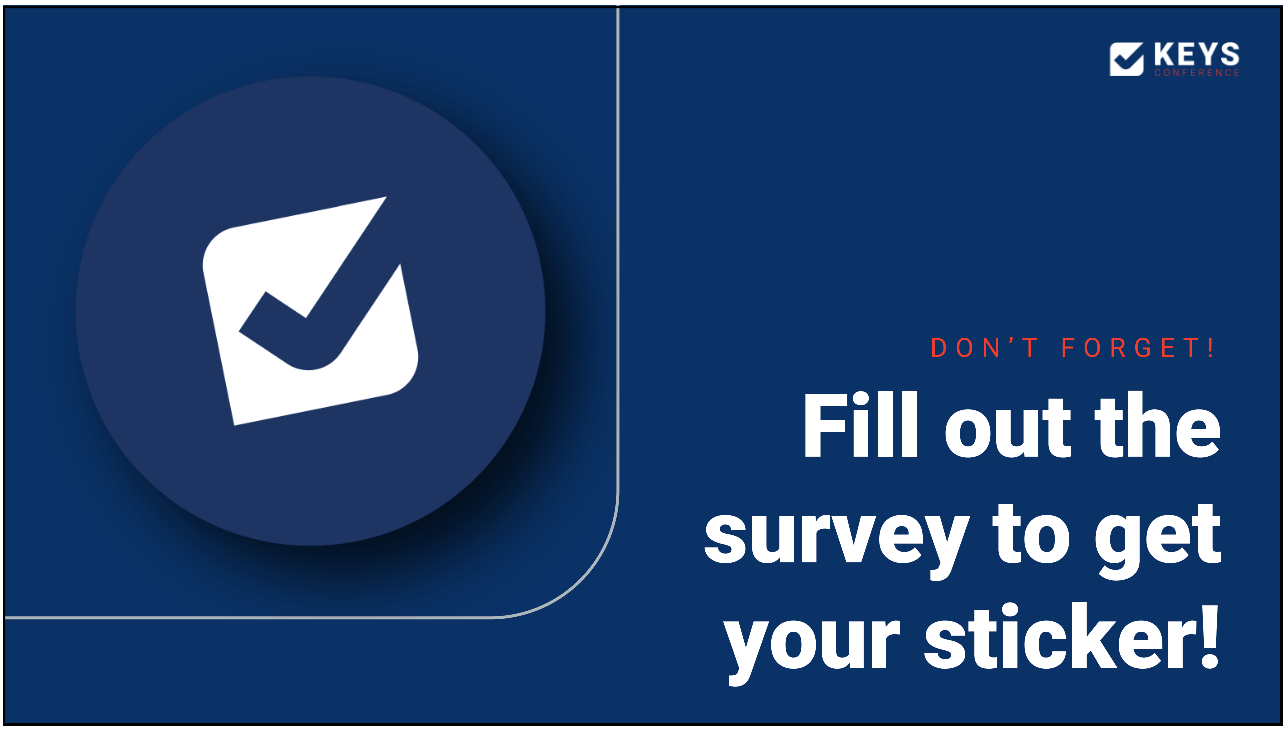
KEYS CONFERENCE

17

18



19



DON'T FORGET!

Fill out the survey to get your sticker!

20

KEYS CONFERENCE

THANKS FOR JOINING!

How to Address the Most Frequently Found Security Issues

Bret Mills & Missy Oliver

Upcoming Sessions

TANDEM

All About Third Parties

Jonathan Garner, Tandem

RISK & COMPLIANCE

7 Ways to Transform How You Report Cybersecurity

Alyssa Pugh, Tandem

CYBERSECURITY

The Human Element of Cybersecurity

BJ Taylor, CoNetrix Security / Boost Consulting

KEYS CONFERENCE