ZYSTON

BEYOND THE ALERT

Pragmatic Compliance

Rebecca (Becca) Allen Diamond, Director of Product, Zyston

ISC2 East Bay 2024 Fall Conference

November 8th, 2024

ISC2 East Bay Chapter

BLUELAVA
MANAGING THE BUSINESS OF SECURITY

Symantec

NASA

ZYSTON
BEYOND THE ALERT

EY

Have our investments in GRC made us safer?

1. Compliance’s Role in the Organization

2. The organization’s approach to compliance

3. The compliance frameworks

Keep me off the sh*t list

Have our investments in GRC made us safer?

Compliance’s Role in the Organization

Embracing a culture of communication moves us closer.

Don’t start with NO

- ✓ Understand the need and tell the business how they can do what they want to do
- ✓ Understand the business drivers and how your compliance program fits in
- ✓ Get away from FUD (Fear, Uncertainty, and Doubt) messaging

Have our investments in GRC made us safer?

Pragmatic

By Definition:

“solving problems in a sensible way that suits the conditions that really exist now, rather than obeying fixed theories, ideas, or rules”*

*Cambridge Dictionary online https://dictionary.cambridge.org/us/dictionary/english/pragmatic

The organization’s approach to compliance

- Business Case
- Risk Case
- Negotiating with your Assesor
- Negotiating with your Business

Have our investments in GRC made us safer?

The organization's approach to compliance

Using risk-based decision-making moves us closer

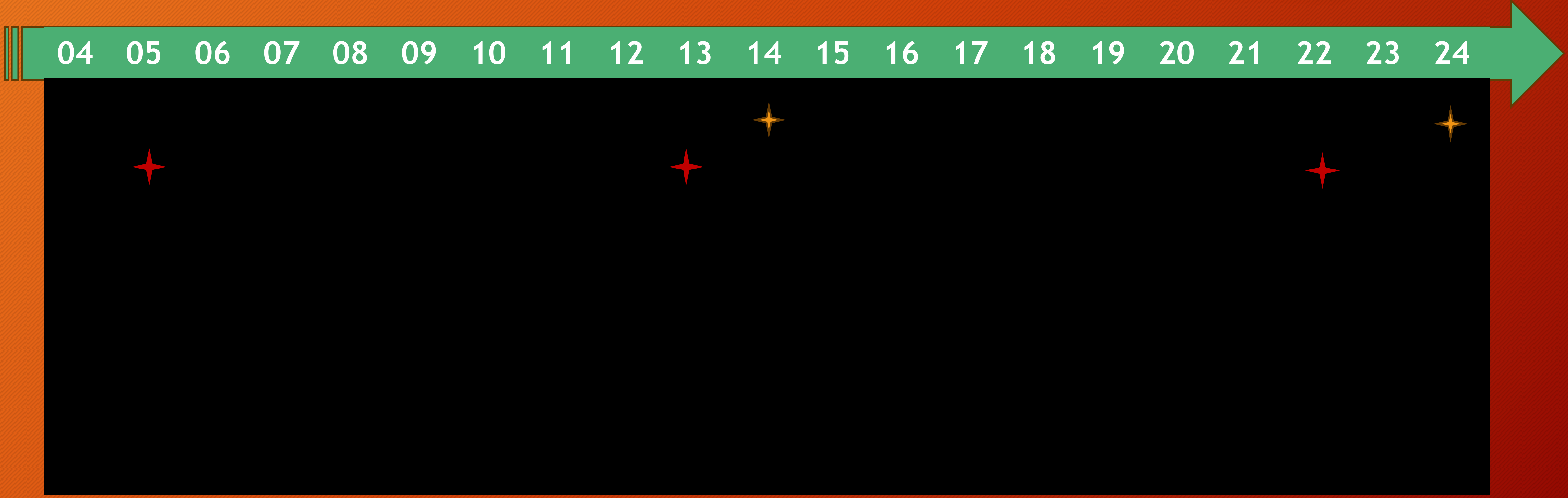
- There is no one "correct" approach
- There will be multiple answers; You may not like any of them
- Evaluate the resources available and realistically determine which approach is best

NIST Cybersecurity Framework (CSF)

04
05
06
07
08
09
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

https://www.nist.gov/cyberframework/history-and-creation-framework

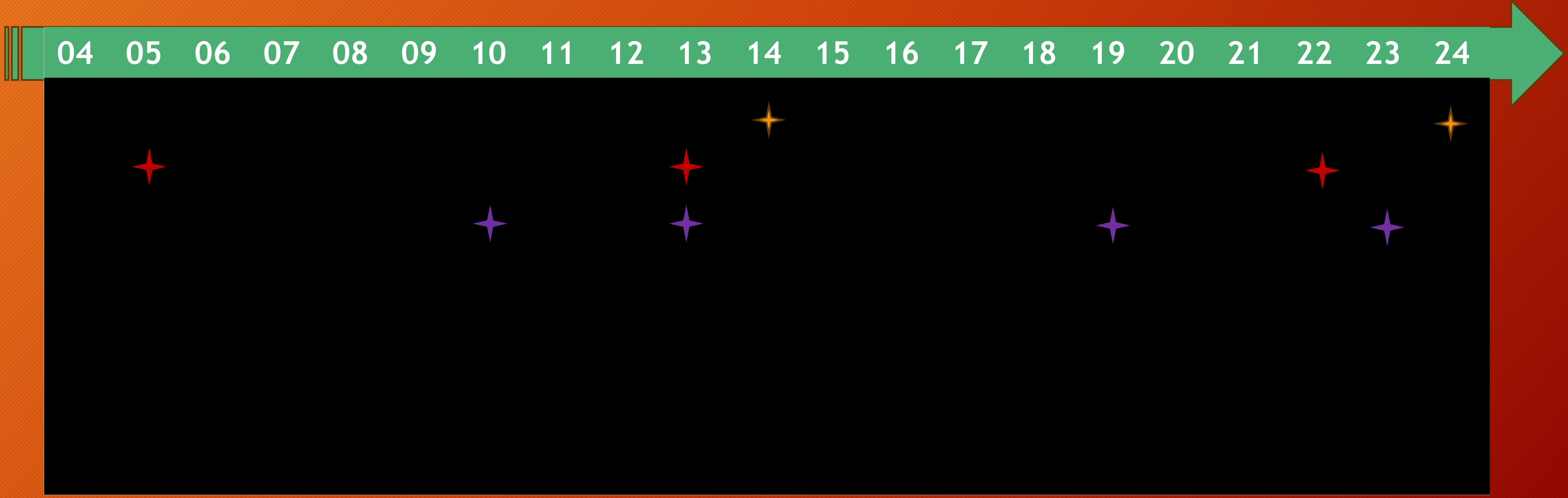
ISO/IEC 27001/27002



04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

https://www.nist.gov/cyberframework/history-and-creation-framework

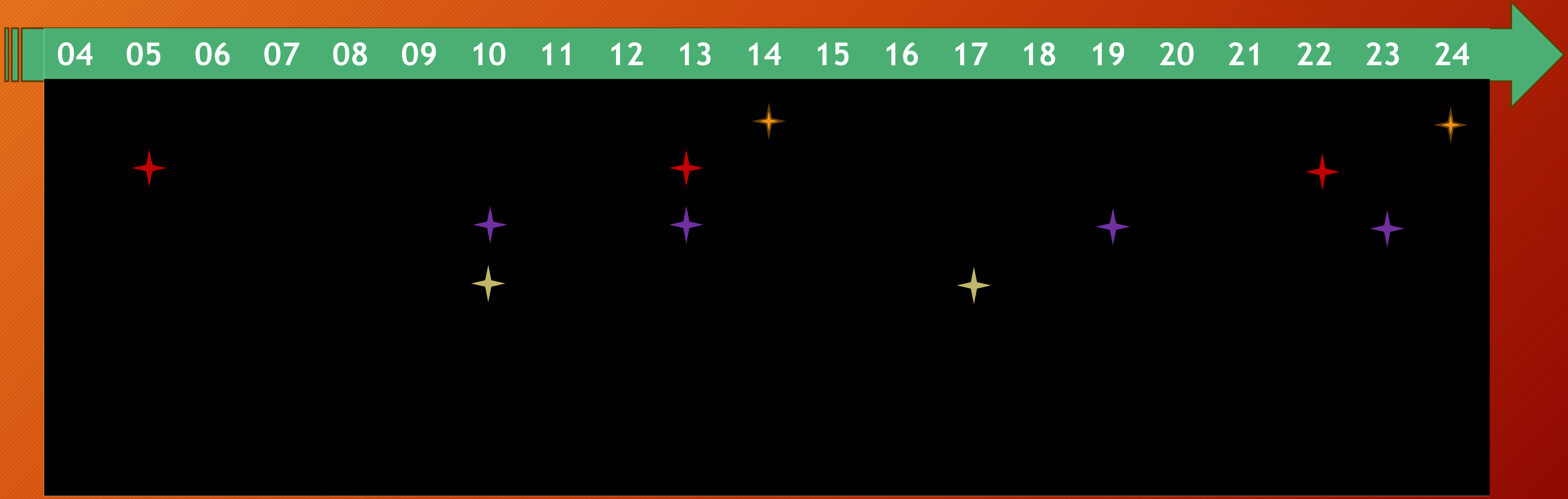
Cloud Security Alliance CCM (Cloud Controls Matrix)



04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

https://cloudsecurityalliance.org/research/artifacts?page=3&term=cloud-controls-matrix

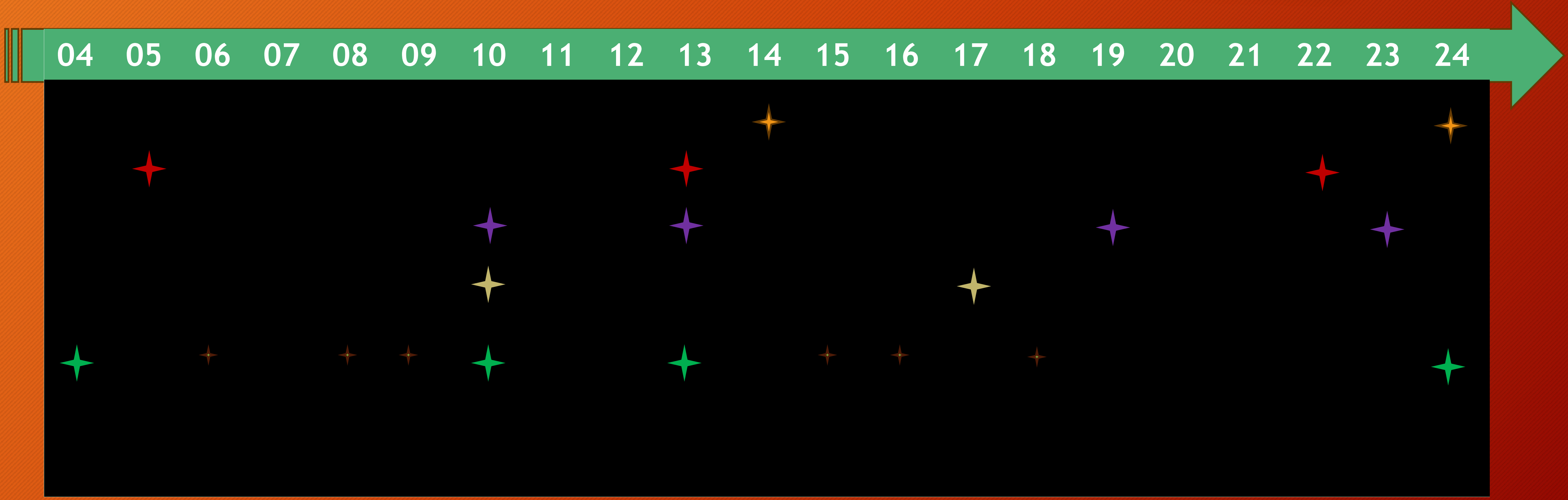
AICPA SSAE 18 SOC 2 Type II



04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

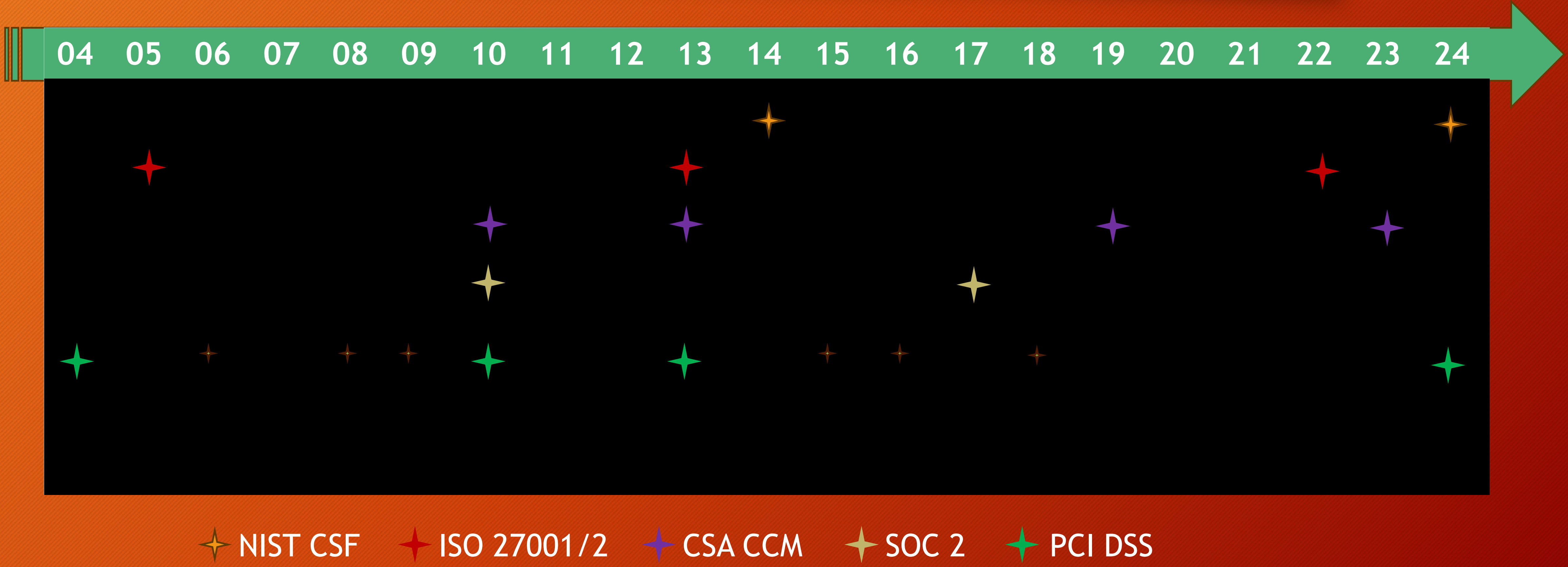
https://secureframe.com/hub/soc-2/history

Payment Card Industry PCI DSS



https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

Framework Modification Timeline



Have our investments in GRC made us safer?

The compliance frameworks are not licensed to drive

A culture of focusing on control intent moves us closer.

Frameworks are not updated at the same pace as technology advancements

Look beyond the narrow view of just the words that make up the control

Dig deep into the control intent and how it applies to your environments

Pragmatic Compliance Makes Us Safer

- ✓ Embrace a culture of communication
- ✓ Use risk-based decision-making
- ✓ Focus on control intent

Thank you