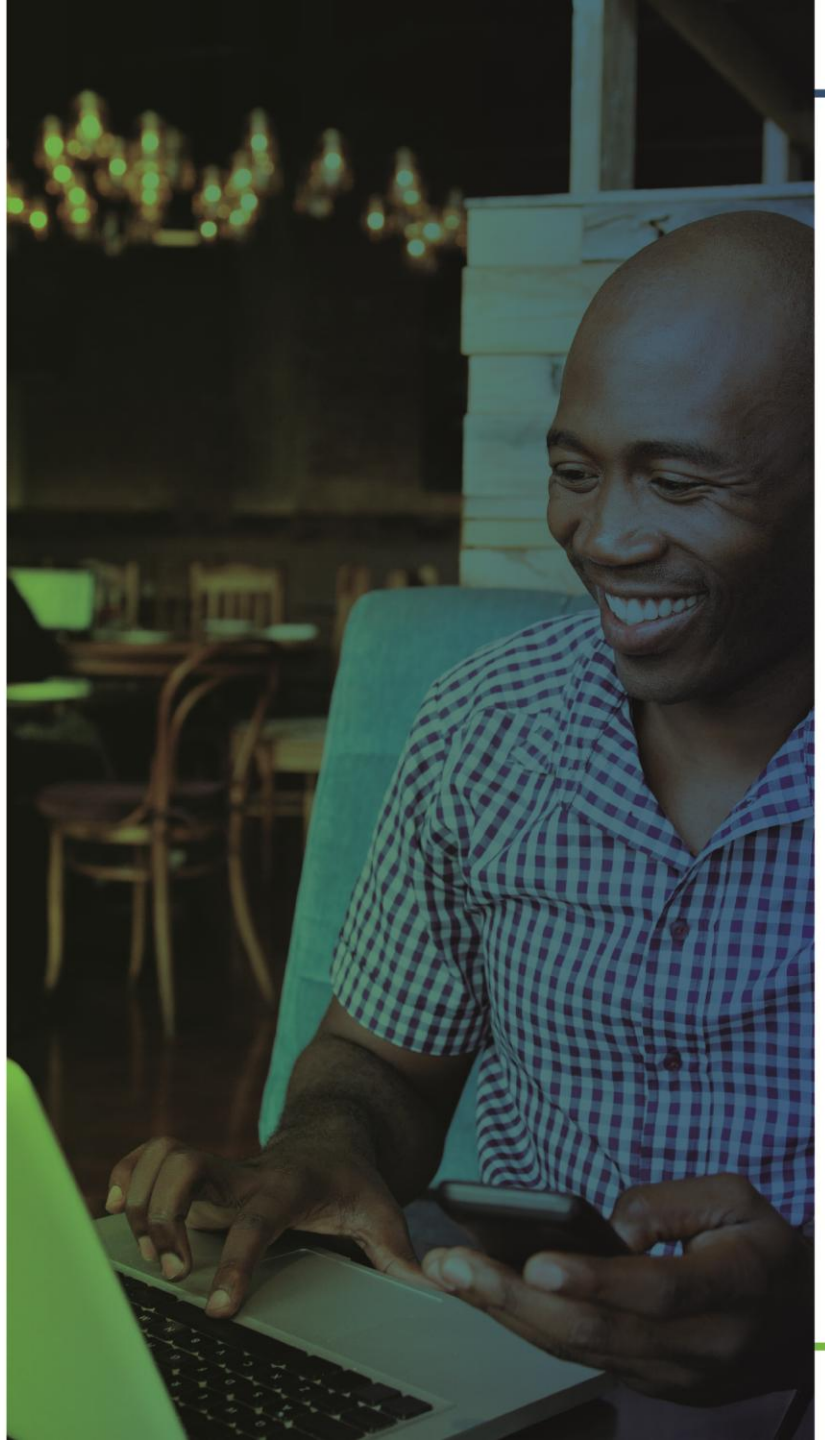


One Size Fits One

Operationalizing with *confidence by design* to optimize privacy, cybersecurity, and AI governance for growth

Tuesday, 17 March
08:00–09:00 PST
11:00–12:00 EST
17:00–18:00 CET

Panelists

Amy Reeder Worley

Managing Director & Data Protection Officer, BRG

Author, *The Confidence Advantage*

Barbara Cosgrove

Vice President, Chief Privacy and Digital Trust Officer

Workday

Frances Palmer-Smith

Chief Privacy Trust Officer

Penumbra, Inc

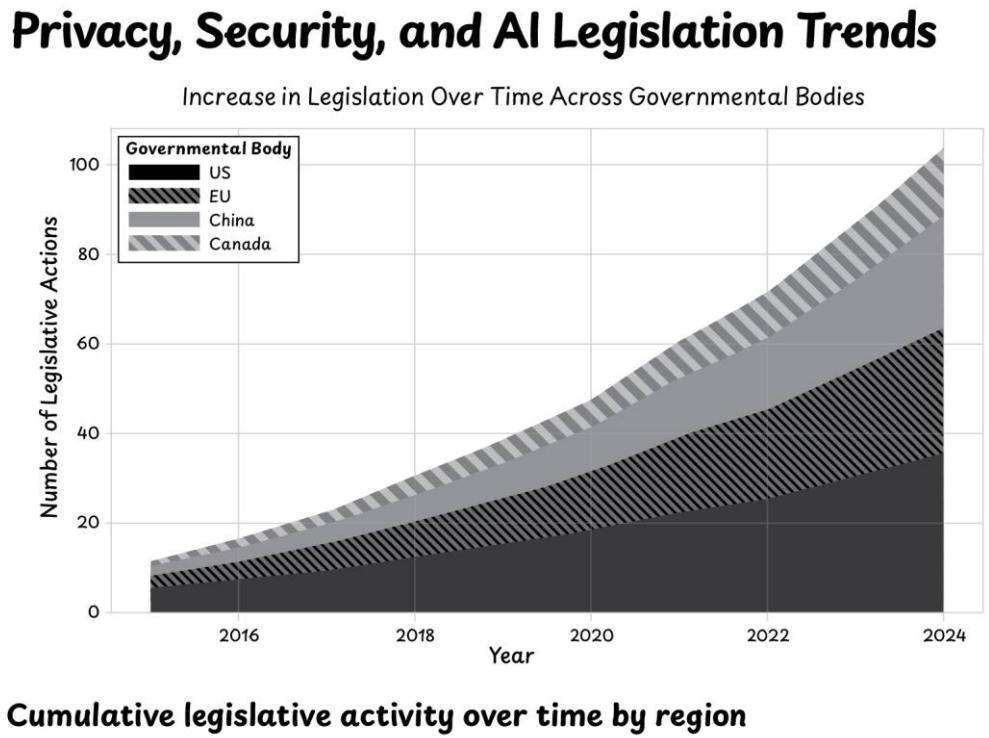
Teresa Troester-Falk

Founder, BlueSky Privacy Stack;

Author, *"So You Got The Chief Privacy Officer Title, Now What?"*

The Problem We're Solving

Legal and Regulatory Complexity and Dynamism



Cumulative legislative activity over time by region

The Value Created by E*vidence-based* Confidence by Design

Poll

Is your business using a cross vertical framework like Confidence by Design to align privacy, cybersecurity, and AI governance under one digital trust banner?

(a) Yes

(b) No

(c) No, but that sounds super cool

The CbD Framework

- Legislation neutral
- Aligns to cyber, privacy, and AI accepted frameworks (NIST/ISO)
- Top down and bottom up- build a culture of confidence around a **shared language** and framework
- Security, Privacy and Responsible AI by Design
- **Multiple implementation methodologies**
- Focuses on accountability, measurement, and culture

Framework allows clear, enterprise-wide understanding of digital risk and opportunity creating accountability

CONFIDENCE BY DESIGN
CONFIDENCE BUILT IN.

PRINCIPLE ONE: We are proactive, not reactive.

PRINCIPLE TWO: We design for transparency and explainability.

PRINCIPLE THREE: We empower users by giving them meaningful control over their data.

PRINCIPLE FOUR: We use data to create value for users and customers, generating positive-sum outcomes rather than zero-sum trade-offs.

PRINCIPLE FIVE: We implement Privacy, Security and Responsible AI by Design.

PRINCIPLE SIX: We practice data minimization.

PRINCIPLE SEVEN: We ensure confidence in our vendors and partners.

PRINCIPLE EIGHT: We hold ourselves accountable.

PRINCIPLE NINE: We design for resilience.

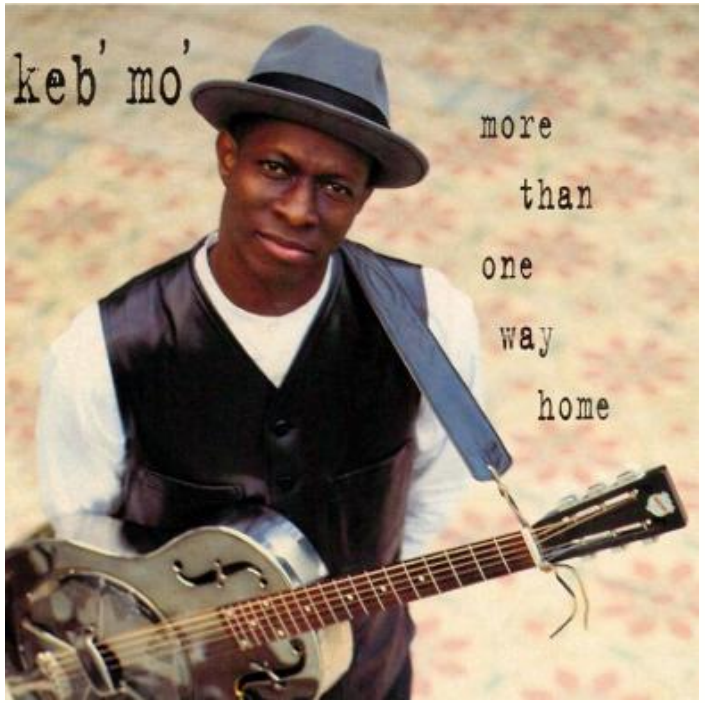
PRINCIPLE TEN: We design for safety and quality.

PRINCIPLE ELEVEN: We design for lawfulness and fairness.

Implementation Structure

There’s more than one way home

IMPLEMENTATOIN: ONE SIZE FITS ONE



"There's more than one way home
Ain't no right way, ain't no wrong
And whatever road you might be on
You find your own way 'cause there's more than one way home"

From Chapter 6

"If someone tells you they can deliver compliance in a box, **run away.** This is true whether the offered solution is software or professional services. **Confidence doesn't come in a box…**

While Confidence by Design works well with heavily control-driven frameworks like, for example, NIST CSF, Secure Controls Framework or SCF…, or ISO 27001, some of its **value is derived from its flexibility**, and the fact that it **can be implemented in any industry vertical under any regulatory regime**."

Poll

Prior to kicking off a major compliance project, have you ever conducted a “premortem”?

(a) Yes

(b) No

(c) I have no idea what you mean

The Pre Mortem

Flexibility as a Feature

- Define what “winning” looks like and understand what is likely to kill “your patient”
- Consider organizational size and structure (hierarchical, flat, start up)
- How regulated is the industry? (retain versus pharma, banking or healthcare)
- Geographic footprint (one country or region or global)
- Budget and resourcing

Potential Structures

- **Option One - The Mega -** Data inventories, policies, procedures, standards operating in a hierarchical model with clear RACIs and lines of accountability
- **Option Two - The Flat -** Inventories for sensitive data, policies, and lots of job aids, guidebooks, and FAQs operating in matrix-like organizations
- **Option Three - The Scrappy -** One or two key policies and risk-focused prioritization of tasks creating bottom-up wins, operating in smaller or less resourced organizations

Poll

Which type of structure do you think would make the most sense for your organization?

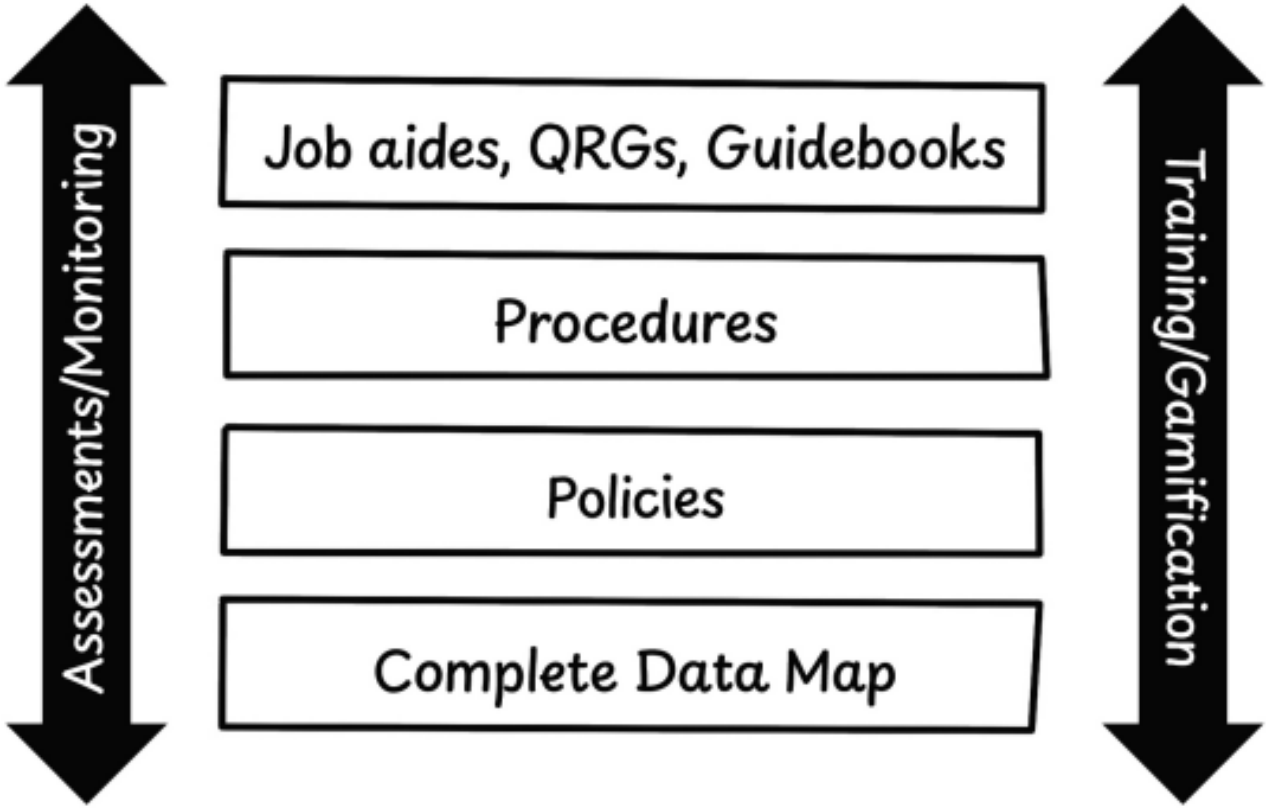
(a) The Mega

(b) The Flat

(c) The Scrappy

(d) Some other creative structural innovation

Possible Confidence by Design Implementation Structure

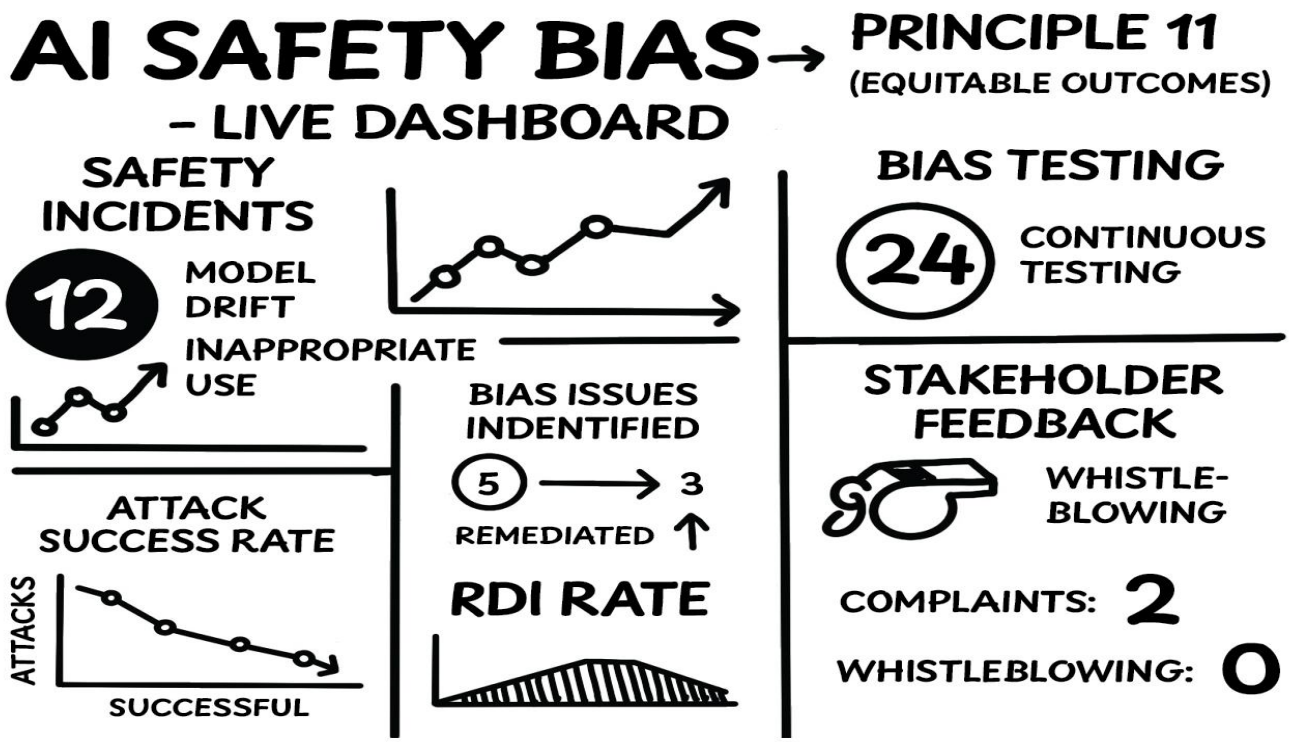


Measuring & Monitoring

You Can’t Know if You’re Winning if You Don’t Keep Score

In an AI-enabled world, monitoring matters

- All the policies and procedures in the world won't create change if you don't identify a desired outcome and test to see if you've achieved it
- **Chpt 9** of the book goes through oodles of monitoring strategies
- What you monitor depends on **the prioritization of your company's risks** and **the structure, size, regulatory profile, and geography of your business**


AI SAFETY BIAS
– LIVE DASHBOARD
PRINCIPLE 11
(EQUITABLE OUTCOMES)
SAFETY INCIDENTS
12
MODEL DRIFT
INAPPROPRIATE USE
BIAS TESTING
24
CONTINUOUS TESTING
BIAS ISSUES INDENTIFIED
5
3
REMEDIATED
STAKEHOLDER FEEDBACK
WHISTLE-BLOWING
ATTACK SUCCESS RATE
ATTACKS
SUCCESSFUL
RDI RATE
COMPLAINTS: 2
WHISTLEBLOWING: 0

RISK ASSESSMENT DASHBOARD

75% of products/services with completed risk assessments

28 indentified risks before deploymnet

114 mitigating controls identified

Quarterly gating reviews in SDLC

SECURITY TESTS PER MONTH

17 PENETRATION TESTING
RED TEAMING

- ☑ VULNERABILITY SCANS
- ☑ CODE SCANS
- ☑ ADVERSARIAL AI

SYSTEMS TESTED

83%

TIME TO PATCH

(MEAN TIME TO REMEDIATE)

29 DAYS

INCIDENT RESPONSE TIME

4 HOURS ⟷ 24 HOURS

TABLETOP EXERCISES CONDUCTED

3 / QTR

1 participant

PATCHING AND UPDATING

SECURITY EVENTS INDENTIFIED

47 SECURITY EVENTS

THIRD-PARTY ASSESSMENTS

B+

- 11 PRIOR
- 6 AFTER

AVG. SCORE
>1 TERMINATED

Building a Confidence Culture

Customers will never love a company until the employees love it first.
–Simon Sinek

Poll

I believe that building a culture of compliance means (choose all that apply)

(a) Training employees on policies and procedures
(b) Messaging from the top of the organization
(c) Celebrating wins, big and small
(d) Creating multimodal learning opportunities and job aids
(e) Create program branding and taglines to drive attention and engagement
(f) Build a volunteer army to create urgency and enable action

Culture

- Compliance and digital trust programs are **competing for attention and "clicks"** just like everything else
- Message must come from as high up in the organization as you can make happen
- Use branding and taglines (channel your inner marketing professional)
- Creative imagery and gamification
- Spot awards
- Bonus and compensation structure

iapp

CONFIDENCE BY DESIGN CHECKLIST

- ☐ Are you planning a project involving personal data or proprietary or trade secret information?
- ☐ Do you want to purchase, deploy, or build an AI system?

Does your project involve:

- ☐ tracking people's behavior?
- ☐ making automated decisions about people?
- ☐ automated scoring of people (applicant ranking, performance reviews)?
- ☐ using AI for HR functions?
- ☐ geolocation, biometric, genetic, or other omic data?

- ☐ Will we share sensitive data with a 3rd party or visa versa?

If you check any 2, reach out to the CbD team.

CONFIDENCE BY DESIGN.

CONFIDENCE BUILT IN.

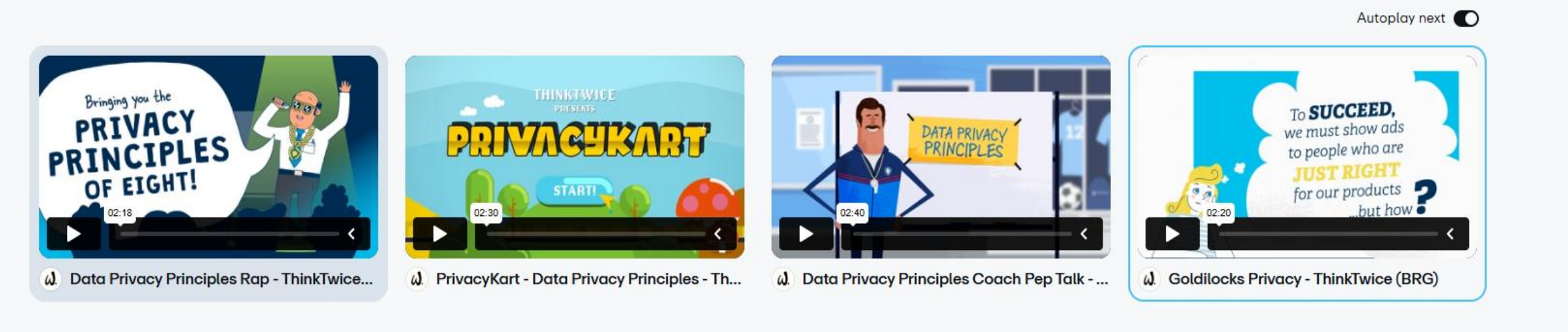
CONFIDENCE BY DESIGN CONFIDENCE BUILT IN.

PRINCIPLE ONE:	We are proactive, not reactive.
PRINCIPLE TWO:	We design for transparency and explainability.
PRINCIPLE THREE:	We empower users by giving them meaningful control over their data.
PRINCIPLE FOUR:	We use data to create value for users and customers, generating positive-sum outcomes rather than zero-sum trade-offs.
PRINCIPLE FIVE:	We implement Privacy, Security, and Responsible AI by Design outcomes rather than zero-sum trade-offs.
PRINCIPLE SIX:	We practice data minimization.
PRINCIPLE SEVEN:	We ensure confidence in our vendors and partners.
PRINCIPLE EIGHT:	We hold ourselves accountable.
PRINCIPLE NINE:	We design for resilience.
PRINCIPLE TEN:	We design for safety and quality.
PRINCIPLE ELEVEN:	We design for lawfulness and transparency.

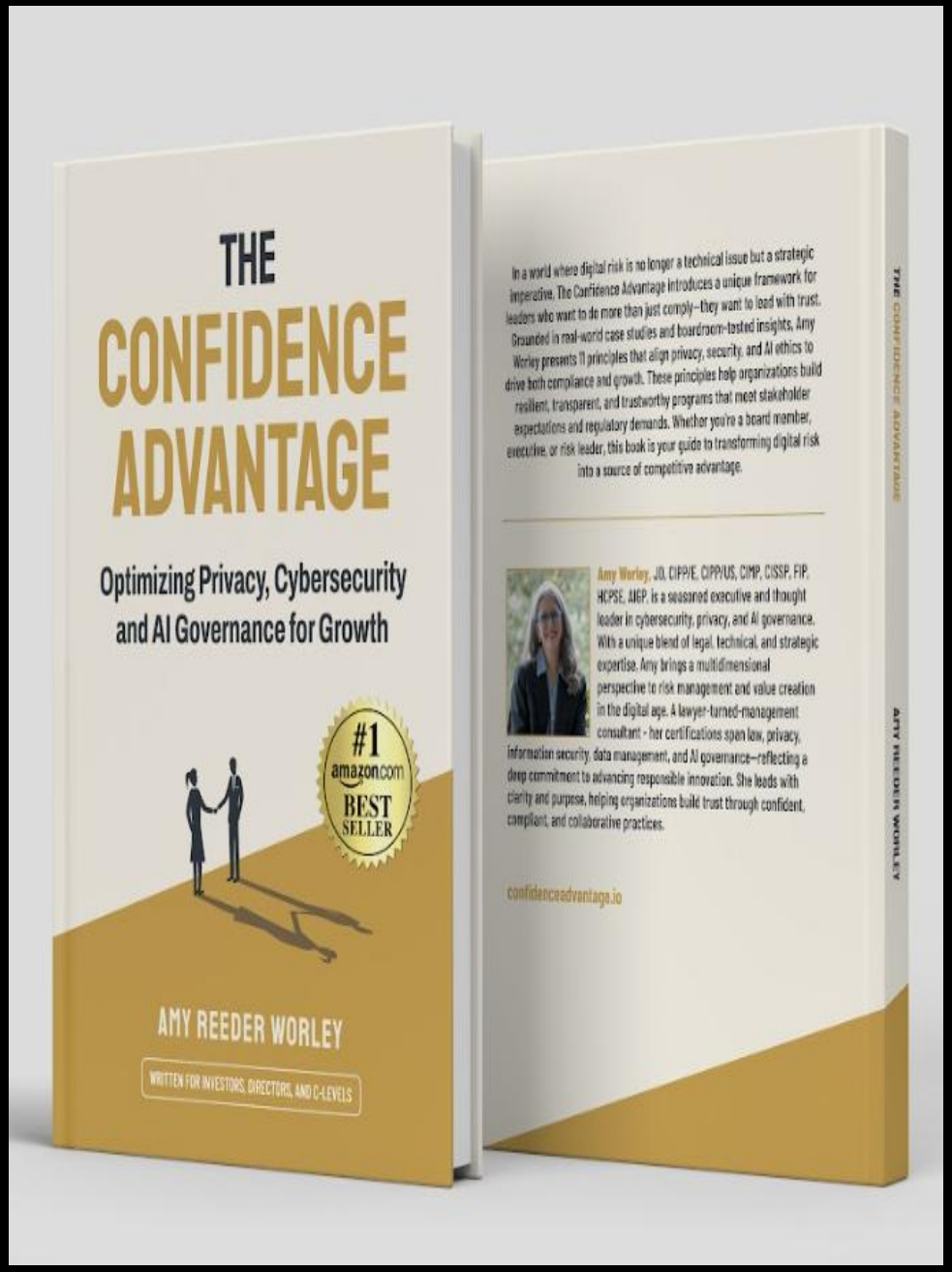
CONFIDENCE BY DESIGN QUIZ GAME

LEADERBOARD

Emma	350
Thuc	280
Aisha	220
Brian	190



[Watch our videos on Vimeo](#).



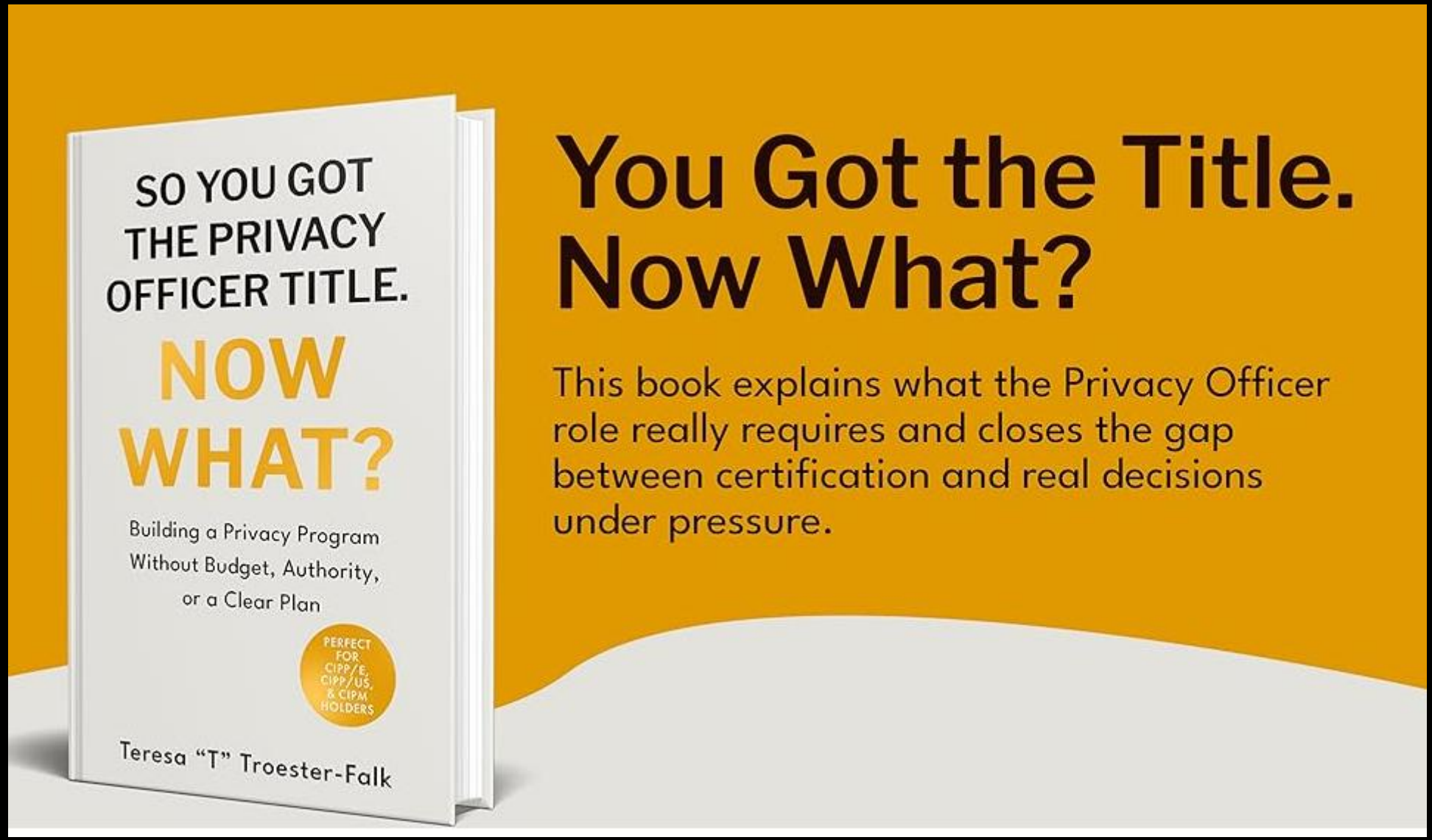
Now Available on Amazon.com

The Confidence Advantage **is available in all formats, hardcover, paperback, and digital. The Audible version will be available in 2-3 weeks!!**

Help us spread the word and share this with your colleagues and executive team. Word of mouth from peers is an excellent way to help show your support.

Thank you for your support.

Also Available on Amazon.com



Teresa's book is available in paperback Hardcopy, and on Kindle.

Visit the website: https://blueskyprivacystack.com/

Sign up for Teresa's excellent privacy substack!

Web Conference
Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here: https://iappwf.questionpro.com/t/AbBPvZ8Bxn

Thank you in advance!

For more information: www.iapp.org

Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your AIGP, CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration prior to the live webinar will automatically receive credit. After the broadcast date, individuals may submit for credit by completing the continuing education application form here: submit for CPE credits.

Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

For questions on this or other IAPP Web Conferences or recordings please contact: **livewebconteam@iapp.org**